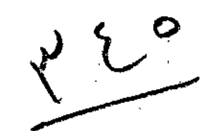
جامعة الإسكندرية
كلية الحقوق



حجيّة الدليل الالكتروني في مجال الإثبات الجنائي
دراسة مقارنة

رسالة مقدمة من الطالبة

عائشة بن قارة مصطفى

للحصول علي درجة الماجستير في الحقوق

إشراف الأستاذ الدكتور

أمين مصطفى محمد
أستاذ ورئيس قسم القانون الجنائي بكلية الحقوق
جامعة الإسكندرية

2009

لجنة المناقشة والحكم على الرسالة

الأستاذ الدكتور: جلال ثروت محمد رئيساً

أستاذ القانون الجنائي بكلية الحقوق جامعة الإسكندرية.

عميد كلية الحقوق ونائب رئيس جامعة الإسكندرية (سابقا)

الأستاذ الدكتور: محمد عيد الغريب عضوا

أستاذ القانون الجنائي بكلية الحقوق

جامعة المنصورة

الأستاذ الدكتور: أمين مصطفى محمد مشرفا وعضوا

أستاذ ورئيس قسم القانون الجنائي بكلية الحقوق

جامعة الإسكندرية


بسم الله الرحمن الرحيم

بسم الله الرحمن الرحيم

﴿ سَنُرِيهِمْ آيَاتِنَا فِي الآفَاقِ وَفِي أَنفُسِهِمْ حَتَّى يَتَبَيَّنَ لَهُمْ أَنَّهُ الْحَقُّ أَوَلَمْ يَكْفِ بِرَبِّكَ أَنَّهُ عَلَى كُلِّ شَيْءٍ شَهِيدٌ ﴾

صدق الله العظيم

آية (53) من سورة فصلت

إهـــــداء

ربّاه... لك خالص حبّي، ورسالتي قربانا.

أمّاه...أنت عذبُ نبعي وما في قلبي لكِ بنيانا.

أبتاه...لكَ عِزّ ونبلُ وللعلمِ رفعة وبنيانا.

رفيق الدّرب قد طال الانتظار ولكن رسالتي ستبدأ بالقِرانا.

أخواتي في الله كنتنّ حلّة الحياة، ولقائي بكنّ أنهار الجنانا.

إلى كلّ من ساعدني خلال إنجازي لهذا البحث من قريب

أو من بعيد، ولو بالكلمة الطيبة ....

أهدي هذا العمل المتواضع

شكر وتقدير

الحمد لله الودود المنّان، الذي منّ علينا بنعمة الإسلام، وبنعمة العلم والكـلام لينطـق اللسان، وهو عاجز عن الإفصاح والبيان، إنّ الكلمات محتارة كيف تـصيغ عبـارة الـشكر والعرفان...كيف وإذا بها ستحدّث عن آلاء الرحمان.. إذ فلنتركها خزينة القلب لعلّـه يقـدّم القربان، بأن يجعل رسالتي هذه خالصة لوجه الرؤوف المنّان وهياما بحبيبنا المصطفى سـيّد ولد عدنان.. .

أمّا شكري الجزيل وأجمل عبارات التقدير فلأستاذي الفضيل الأستاذ الدكتور " **أمـين مصطفى محمّد**"، الذي لم يبخل عليّ بتوجيهه الرشيد، وتقويمه السديد إلى أن خرج إلى النور هذا العمل بصورته الحاليّة، وما هذا كلّه إلاّ بفضل ومنّ من خالق عزيز حميد.. .

ولو ظلّ المداد يخط وينسج أسمى آيات الشكر والعرفان لعالمنا الجليل الأستاذ الدكتور "**جلال ثروت**"، فلا أظن أن يُعرف له نفاد، لأنّه سيظل منارة العلم إلى أن يأتي يـوم الثنـاء، ليناديه المولى جلّ وعلا عبدي ها قد وفيّت، فجزائي وعطائي لك اليوم ما له نفاد.

إي وربي إنّه لشرف لي عظيم أن تكون رسالتي بين يدي أستاذ جليل كبير، بل وحقيق عليّ أن أقول قد عزّ له النظير..

وجدير بالشكر والتقدير أستاذنا الكريم، الأستاذ الدكتور "**محمّد عيد غريـب** " قبولـه الاشتراك في لجنة المناقشة والحكم علي هذه الرسالة، وما هذا لما للعلم عندهم مـن شـرف ونبالة، فله منّي فائق الاحترام والتقدير.

وأغتنم عبارات شكري وتقديري بباقة غنّاء، بالبلسم والزهـراء، للـوردة البيـضاء، والدتي لصبرها الجميل على هذا البعد الطويل.

ووالدي الجليل على حلمه الذي ما له بديل، فلهم منّي أسمى عبارات الحب والتقدير.

ولكلّ من ساهم في نجاح رسالة مخلصة لوجه العليّ القدير.

الباحثة

مقدمة

1- موضوع الدراسة:

يشهد العالم منذ منتصف القرن العشرين ثورة جديدة، اصطلح على تسميّتها بالثورة المعلوماتيّة [1]، وذلك إشارة إلى الدور البارز الذي أصبحت تلعبه المعلومات في الوقت الراهن، فقد أمست قوّة لا يستهان بها في أيدي الدول والأفراد. وكان التطوّر الهائل الذي شهده قطاعي تكنولوجيا المعلومات والاتصالات والاندماج المذهل الذي حدث بينهما فيما بعد هو المحور الأساسي الذي قامت عليه هذه الثورة.

وممّا لاشك فيه أنّ الثورة المعلوماتيّة ونتيجة للتقنيات العالية التي تقوم عليها والتي تتمثّل في استخدام الحواسيب والشبكات المعلوماتيّة ـ خاصّة شبكة الانترنت [2]ـ التي تربط بينها، قد تركت آثارا ايجابيّة وشكّلت قفزة حضاريّة ونوعيّة في حياة الأفراد والدول، حيث تعتمد القطاعات المختلفة في الوقت الحالي في أداء عملها بشكل أساسي على استخدام الأنظمة المعلوماتيّة نظرا لما تتميّز به من عنصري السرعة والدقّة في تجميع المعلومات وتخزينها ومعالجتها ومن ثمّ نقلها وتبادلها بين الأفراد والجهات والشركات والمؤسسات المختلفة داخل الدولة الواحدة أو بين عدّة دول. كما أصبحت هذه الأنظمة مستودعا لأسرار الأشخاص المتعلّقة بحياتهم الشخصيّة أو بطبيعة أعمالهم الماليّة والاقتصاديّة، كذلك أمست مستودعا لأسرار الدول الحربيّة والصناعيّة والاقتصاديّة التي تعبّر على قدر من الأهميّة والسريّة.

إلاّ أنّ هذا الجانب الايجابي المشرق لعصر المعلوماتيّة لا ينفي الانعكاسات السلبيّة التي أفرزتها هذه التقنيّة والمتمثّلة في إساءة استخدام الأنظمة المعلوماتيّة واستغلالها على نحو غير مشروع وبصورة تضرّ بمصالح الأفراد والجماعات وبالتالي بمصلحة المجتمع كلّه، حيث أدّى هذا التطوّر الهائل إلى ظهور أنماط مستحدثة من الجرائم اصطلح على تسميّتها بالجرائم الالكترونيّة.

---

[1] كلمة معلوماتيّة (informatique) هي اختصار مزجي لكلمتي معلومة(information) وكلمة آلي أو آلية (automatique)، وهي تعني المعالجة الآلية للمعلومة(Traitement automatique de l'information)، انظر: أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربيّة، القاهرة، 2000، ص 270.

[2] الانترنت : عبارة عن شبكة تتألف من العديد من الحاسبات الآليّة المرتبطة ببعضها البعض، إمّا عن طريق خطوط التلفون أو عن طريق الأقمار الصناعيّة، وتمتدّ عبر العالم لتؤلّف في النهاية شبكة هائلة، بحيث يمكن للمستخدم لها(user) الدخول من أيّ مكان في العالم وفي أيّ وقت،طالما كان جهاز الحاسب الآلي مزوّدا بمودم (modem) يربطه بخط الهاتف لتلقي وإرسال البيانات عبر مزوّد الخدمة (Service Provider). انظر: د/ جميل عبد الباقي الصغير، الانترنت والقانون الجنائي، الأحكام الموضوعيّة للجرائم المتعلّقة بالانترنت، الطبعة الأولى، دار النهضة العربيّة، 2001، ص 4.

وخطورة هذه الظاهرة الإجراميّة المستحدثة تتجلى في سهولة ارتكابها، وأنّ تنفيذها لا يستغرق إلاّ دقائق معدودة، وأحيانا تتمّ في بضع ثوان، وأنّ محو آثار الجريمة وإتلاف أدلتها غالبا ما يلجأ إليه عقب ارتكاب الجريمة، فضلا عن أن مرتكبيها يتّسمون بالدهاء والذكاء، وغالبا ما يلجؤون إلى تخزين البيانات المتعلقة بأنشطتهم الإجراميّة في أنظمة الكترونية داخل دول أجنبيّة بواسطة شبكة الاتصال عن بعد، مع استخدام شفرات أو رموز سريّة لإخفائها عن أعين أجهزة العدالة، ممّا يثير مشكلات كبيرة في جمع الأدلة الجنائيّة وإثبات هذه الجرائم قبلهم.

وعلى ضوء ذلك، فإنّ كشف ستر هذا النوع من الجرائم يحتاج إلى طرق الكترونيّة تتناسب مع طبيعته بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة، تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنيّة والعلميّة، ومن تمّ نسبتها إلى فاعليها، وتدعى هذه الوسيلة **بالدليل الالكتروني** **(Electronic evidence)**.

وتجدر الإشارة إلى أنّ تأثير التطور التكنولوجي لا يقف عند مضمون الدليل، وإنّما يمتدّ هذا التأثير كذلك إلى الإجراءات التي يترتّب عليها الحصول على هذا الدليل، ولذلك يجب أن تكون هذه الإجراءات المتطوّرة ذات طبيعة مشروعة لكي تحافظ على مشروعيّة الأدلّة المتولدة منها.

2ـ أهميّة الموضوع:

1ـ لموضوع الدليل الالكتروني ومدى حجيّته في الإثبات الجنائي أهميّة بالغة، كانت دافعا لاختياره وتناوله بالبحث والدراسة، وتظهر هذه الأهميّة من خلال ارتباطه الوثيق والمباشر بظاهرة جديدة وهي الجرائم الالكترونيّة، التي بدأت في الظهور والانتشار حاليا، حيث تعتبر من المواضيع الشائكة التي بدأت تشغل فكر فقهاء القانون الجنائي، ولعلّ خير دليل على ذلك كثرة المؤتمرات الدوليّة والاتفاقيات التي أبرمت في سبيل مكافحة الجريمة الالكترونيّة سواء على المستوى الدولي أو المحلي[1].

---

[1] المؤتمر الدولي لحقوق الإنسان بطهران المنعقد في الفترة الممتدة من 22 أبريل إلى 13 مايو عام 1968، و الخاص بأثر التقدم التكنولوجي على حقوق الإنسان . وفي 28 يناير 1981 تمّ التوقيع على اتفاقية متعلقة بحماية الأشخاص في مواجهة المعالجة الالكترونية للمعطيات الشخصية، وكانت تحت إشراف المجلس الأوربي، كما قام هذا الأخير بإصدار التوصية رقم 95(13) في 11ـ 09ـ1995 ، والتي تتعلق بمشكلات الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات. وفي 23 نوفمبر 2001 ، شهدت العاصمة المجرية بودابست أولى المعاهدات الدولية التي تكافح الجرائم الالكترونيّة، حيث وقّع عليها ثلاثون دولة بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأوربي وهي كندا واليابان وجنوب إفريقيا والولايات المتحدة==

ولذلك فإذا استطاع الجناة تطوير طرق الإجرام على هذا النحو من التقنيّة العالية في بيئة تكنولوجيا المعلومات، كان من الضروري تطوير وسائل الإثبات بما يواكب التطور في وسائل الإجرام الالكتروني، وأصبح متطلبا من أجهزة العدالة الجنائيّة أن تتعامل مع أشكال مستحدثة من الأدلة في مجال الإثبات الجنائي، خاصّة مسألة قبول وحجيّة الدليل الالكتروني، وهذا الأخير كان إحدى المسائل الهامّة التي تتعرّض لها المؤتمرات الدوليّة، حيث كان الموضوع الرئيسي للمؤتمر الدولي الخامس عشر للجمعيّة الدوليّة لقانون العقوبات، الذي عقد في ري ودي جانيرو بالبرازيل في الفترة من (4 ــ 6 سبتمبر 1994)، كما أنّ هذه المسألة أيضا كانت محلّ بحث في (الحلقة التمهيديّة) التي عقدت على المستوى الدولي في فيوربخ (Würzburg) بألمانيا في الفترة من (5ــ 8 أكتوبر 1992)، وحديثا أصدرت الأمم المتّحدة مرشدا عاما حول مكافحة والحدّ من الجرائم الالكترونيّة في يناير 2000 [1].

أمّا على مستوى العالم العربي، فلم تكن هناك جهود كبيرة في مجال مكافحة هذه الجرائم المستحدثة، سوى بعض الجهود العلمية، والأمنية بشكل خاص، حيث أصبحت متوالية في مجال رصد وتتبع الظواهر الأمنية المصاحبة لانتشار الحاسبات والانترنت، ولعلّ آخرها المؤتمر العلمي الأوّل حول العالم الرقمي وجرائم الشبكات الالكترونيّة، الذي شهدته العاصمة المصرية – القاهرة – في الفترة من(4- 5 مارس 2009) وتناول لأوّل مرّة بالدراسة مسألة الإثبات الجنائي باستخدام الوسائل الالكترونيّة، ومدى قبول الدليل الالكتروني في الإثبات الجنائي [2].

==الأمريكية. وحاليا مازالت المشاورات بشان تشكيل مجموعة عمل تُعنَى بالإجرام الالكتروني مستمرة وكانت هذه المشاورات قد أخذت شكلا جديدا في أعقاب المرحلة الأولى من القمّة الدولية بشان مجتمع المعلومات (WSIS) في جنيف نهاية ديسمبر 2003، ثمّ نوقشت باستفاضة في المرحلة الثانية من القمّة في تونس نهاية نوفمبر 2005.

[1] International Review of Criminal Policy، United Nation " Manual on the Prevention and Control of computer related Crime 2000". Available at: http://www.ifs.univie.ac.at/pr2gq1/rev434.html .

[2] ناقش المؤتمر العلمي الأوّل حول العالم الرقمي وجرائم الشبكات الالكترونيّة، عددا من الموضوعات تتعلق بصفة عامة بالمواجهة الموضوعيّة والإجرائية للجرائم الالكترونيّة، وجاء ذلك في ستّة محاور تتمثّل فيما يلي: **المحور الأوّل**، عبارة عن مقدّمة تقنيّة وقانونية عن الجريمة الالكترونيّة، حول كيفية اختراق الشبكات مثلا وغيرها من الأساليب الفنيّة المستخدمة في ارتكاب الجريمة المعلوماتيّة...، أمّا **المحور الثاني**، فجاء عبارة عن رصد لأهمّ الأنماط التقليديّة للجريمة الالكترونيّة، كالقذف والسب والاعتداء على حرمة الحياة الخاصّة عبر الانترنت، والإرهاب الالكتروني..، أمّا **المحور الثالث**، فقد خصّص لدراسة الجرائم المتعلّقة بالمحتوى، كالاعتداء على الملكيّة الفكريّة والاعتداء على حقوق البث الرقمي للقنوات الفضائيّة..، أمّا **المحور الرابع**، فجاء خاصّا بالجرائم المتعلّقة بالآداب العامّة، كالاستغلال الجنسي للأطفال من خلال شبكة الانترنت،==

2 ــ وتبرز أهميّة الموضوع كذلك، في أنّه تناول أحدث الوسائل العلميّة وأكثرها انتشارا في قضايا الإثبات الجنائي، تلك الوسائل التي جاءت لتلاءم التطورات التكنولوجية والتقنيّة التي تطوّر معها الفكر الإجرامي، فكر الجرائم الالكترونيّة، ممّا ألقى على عاتق القائمين على مكافحة الجريمة في الدولة عبئا شديدا ومهاما جساما تفوق القدرات المتاحة، لهم وفق أسس وقواعد إجراءات البحث الجنائي والإثبات الجنائي التقليديّة، نظرا لعدم كفاية، وعدم ملائمة هذه النظم التقليديّة في إثبات تلك الجرائم سواء من الناحيتين القانونيّة أو التقنيّة، وكان على المشرّع حتميّا أن يستحدث من التشريعات ما يلائم هذا النوع من الجرائم، فضلا عن إنشاء أجهزة فنيّة متخصّصة يناط بها عمليّة الإثبات العلمي الفني لهذه الجرائم.

3 ــ وتكمن أهميّة البحث أيضا في محاولته بيان مدى تأثير طبيعة الدليل على اقتناع القاضي الجنائي، حيث أصبح القاضي الجنائي حاليّا يستند على الدليل العلمي بما فيه الدليل الالكتروني باعتباره تطبيقا من تطبيقات الدليل العلمي، ممّا جعل للخبير الدور الأكبر في السيطرة على العمليّة الإثباتيّة، مقابل تضاؤل دور القاضي الجنائي في تقديره لقيمة الدليل الالكتروني.

4 ــ وأخيرا، إذا كان العلم قد أحدث الكثير من وسائل الإثبات، كالدليل الالكتروني وأمدّ سلطات التحقيق بوسائل علميّة حديثة ومتطوّرة، فإنّ اقتناع القاضي في الأمور الجنائيّة، يأتي كوجاء يحمي من الشطط، التي ترتبت على الوسائل العلميّة الحديثة في الإثبات، والتي في كثير من الأحيان تكون في ذاتها اعتداء على الحياة الخاصّة للأفراد. ذلك ما سنحاول بيانه في هذه الدراسة إنشاء الله.

3ـ إشكالات البحث:

بالنظر إلى الطبيعة الخاصة التي يتميّز بها الدليل الالكتروني، وما قد يصاحب الحصول عليه من خطوات معقّدة، فإنّ قبوله في الإثبات كدليل جنائي قد يثير العديد من المشكلات، فكما سنعلم أنّ مستودع هذه الأدلّة هو الوسائل الالكترونيّة، ولذلك فيمكن التلاعب فيها وتغيير الحقيقة التي يجب أن تعبّر عنها.

==وتسهيل الدعارة عبر الانترنت...، وخصّص **المحور الخامس**، بالجرائم الماسّة بشبكة المعلومات الدوليّة، كالدخول غير المشروع على الشبكة، والاعتداء على قواعد البيانات وبنوك المعلومات. أمّا **المحور السادس والأخير**، فخصّص للمواجهة الإجرائيّة لهذه الجرائم المستحدثة، من خلال بيان كيفيّة تعامل مأموري الضبط القضائي مع الدليل الرقمي، بالإضافة إلى مسائل الضبط، التفتيش والمعاينة في البيئة الالكترونيّة، ومدى حجيّة الدليل الرقمي في الإثبات الجنائي.

ولذلك فإن المشكلات التي يثيرها هذا الدليل ليس بسبب أنه قد يصلح ليكون وسيلة من وسائل الإثبات الجنائي أم لا فحسب؟ وإنما تتعلق أيضا بها في: كيف نضمن مصداقية هذه الأدلة وأنها تعبر بالفعل عن الحقيقة التي تهدف إليها الدعوى الجنائية. هذا من جهة.

وعلى ذلك، يتطلب الإجابة على إشكالية البحث ردّها إلى عناصرها الأوليّة طبقا للتساؤلات التاليّة:

1. كيف يمكن استخراج دليل الكتروني بوصفه دليل إثبات أمام القضاء؟.
2. فهل تكفي القواعد الإجرائيّة المقرّرة للجرائم التقليديّة لكي تسري على الجرائم الالكترونيّة؟
3. ما هي الشروط اللازمة لاعتماد الدليل الالكتروني كدليل إثبات في الجرائم الالكترونيّة؟.
4. مدى اقتناع القاضي الجنائي بالدليل الالكتروني؟.

4ـ الصعوبات التي يطرحها موضوع البحث:

لا يفوتنا في هذا المقام أن نذكر أنّ ثمّة صعوبات كانت عائقا أمامنا في إعداد هذا البحث، وقد تمثّلت في اختيار موضوع البحث، وذلك كون موضوع البحث: "حجّيّة الدليل الالكتروني في مجال الإثبات الجنائي"، موضوعا حديثا لم يسبق بحثه بتعمق من الناحيّة الجنائيّة بالتحديد ولو أنّ هناك مجموعة من المقالات والمراجع التي عالجت الموضوع من الناحية المدنية أو التجارية، أو حتّى الجنائيّة ولكن بشكل جزئي أي دون تناول كل جوانبه، أو أنّها عالجته بشكل سطحي.

بالإضافة إلى ذلك، ارتباط الجرائم محل الدراسة بالحاسب الآلي، ممّا يتطلب الإحاطة بمكونات هذا الأخير وبنظام المعالجة الآلية للمعطيات وبالشبكات، وبطرق الدخول، وكل ما يتعلق بهذه الجرائم من تقنيات، وهذا يحتاج إلى جهد فني فضلا عن الجهد القانوني .

5 ـ منهج البحث:

حرصنا على أن ننتهج في دراستنا هذه سبيلا منطقيّا يسير جنبا إلى جنب مع تسلسل الفكرة حرصا على بلوغ الغاية من الدراسة، لذلك اتّبعنا منهجا ذا ثلاث أبعاد، فهو منهج تأصيلي، تحليلي ومقارن.

منهج تأصيلي أوّلا، لأنّه يرد النقاط التفصيليّة إلى أصولها النظريّة، وفي دراستنا هذه نرجعها إلى النظرية العامة للإثبات الجنائي.

وتحليليّ ثانيًا، من خلال قيامنا بشرح الموضوعات المختلفة التي عالجناها في هذه الدراسة، كتحليل أسباب صعوبة إثبات الجريمة الالكترونيّة، وإيراد تطبيقات قضائيّة عليها واستخلاص النتائج التي تترتّب على ذلك التحليل.

أمّا المنهج المقارن، فيظهر جليًا من خلال مقارنة النظام اللاتيني وعلى قمّته دراسة القانون الفرنسي وقوانين أخرى التّي تأثّرت به كالقانون الجزائري والمصري، مع النظام الانجلو أمريكي من خلال دراسة القانون الأمريكي والانجليزي، باعتبار هذه القوانين الأخيرة أيقنت بسلامة منطق الأدلة الالكترونيّة ومنظورها العلمي.

6- خطّة البحث:

من أجل معالجة الإشكاليات السابق طرحها، ارتأينا تقسيم هذا البحث إلى قسمين دون أن يسبقهما مبحث تمهيدي، حيث تطرقنا في الفصل الأوّل لدراسة ماهية الدليل الالكتروني، فقمنا بتقسيمه إلى مبحثين خصصنا الأوّل منه للحديث عن ذاتية الدليل الالكتروني، وأفردنا الثاني لدراسة إجراءات جمع الدليل الالكتروني.

وتناولنا في الفصل الثاني بحث مدى اقتناع القاضي الجنائي بالدليل الالكتروني، وقسّمناه هو الآخر إلى مبحثين: مبحث تكلّمنا فيه عن سلطة القاضي الجنائي في قبول الدليل الالكتروني. وآخر لدراسة سلطة القاضي الجنائي في تقدير الدليل الالكتروني.

وفي آخر الدراسة توصّلنا لعدد من النتائج والتوصيات يمكن اقتراحها في هذا الموضوع، تمّ إدراجها في خاتمة هذا البحث.

وعليه تكون الخطّة كالتالي:

مقدمة

الفصل الأول: ماهية الدليل الالكتروني.

المبحث الأوّل: ذاتيّة الدليل الالكتروني.

المطلب الأول: محل الدليل الالكتروني(الجريمة الالكترونيّة).

المطلب الثاني: مفهوم الدليل الالكتروني.

المبحث الثاني: إجراءات جمع الدليل الالكتروني.

المطلب الأول: الإجراءات التقليديّة لجمع الدليل الالكتروني.

المطلب الثاني: الإجراءات الحديثة لجمع الدليل الالكتروني.

الفصل الثاني: مدى اقتناع القاضي الجنائي بالدليل الالكتروني

المبحث الأوّل: سلطة القاضي الجنائي في قبول الدليل الالكتروني.

المطلب الأول: أساس قبول الدليل الالكتروني في الإثبات الجنائي.

المطلب الثاني: القيود الواردة على حريّة القاضي الجنائي في قبول الدليل الالكتروني.

المبحث الثاني: سلطة القاضي الجنائي في تقدير الدليل الالكتروني.

المطلب الأول: حريّة القاضي الجنائي في الاقتناع بالدليل الالكتروني.

المطلب الثاني: الضوابط التي تحكم اقتناع القاضي بالدليل الالكتروني.

خاتمة.

الفصل الأوّل
ماهيّة الدليل الالكتروني

ممّا لا شكّ فيه أنّ الثورة العلميّة في مجال نظم المعلومات الالكترونية لم تؤثّر فقط في نوعية الجرائم التي ترتّبت عليها وفي نوعية الجناة الذين يرتكبون هذه الجرائم، وإنّما أثرت تأثيرا كبيرا على الإثبات الجنائي، خاصّة على طرق هذا الإثبات، حيث يمكن القول أن الطّرق التقليدية أصبحت عقيمة بالنسبة لإثبات هذا النوع من الجرائم المستحدثة، لذلك ظهر نوع خاص من الأدلة يمكن الاعتماد عليه في إثبات الجريمة الالكترونيّة، ومن ثمّ نسبتها إلى فاعليها، وهو ما يعرف **بالدليل الالكتروني أو الرقمي**[1]، ونحن في دراستنا آثرنا ترجيح مصطلح الدليل الالكتروني(Electronic evidence) على اعتبار أنّه اللفظ المستخدم من طرف المشرع الأوربي في التوصية رقم (95) 13 الخاصة بمشاكل الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات والتّي تمّ اعتمادها من قبل لجنة الوزراء في(11 — 09 — 1995)[2]، كذلك تمّ استعمال هذا المصطلح في الفقرة الثانية من المادة (14) من اتفاقية بودابست الموقعة في (23 نوفمبر 2001) [3]، كما جاء هذا الوصف أيضا في عنوان المرشد الفيدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية لسنة 1994 [4].

---

(1) يرجع أصل مصطلح الدليل الرقمي (Digital evidence) إلى استخدام النظام الرقمي الثنائي **1، (0)** وهي الصيغة التي تسجل بها كل البيانات (أشكال وحروف و رموز و غيرها) داخل الحاسب الآلي، حيث يمثل **(الصفر)** وضع الإغلاق **Off**، والواحد (1) وضع التشغيل **On**، ويمثل الرقم **صفر(0)** أو الرقم واحد **(1)** ما يعرف بالبيت (Bit)، ويشكل عدد8 بيت(Bits) ما يعرف بالبايت **Byte**. انظر: بيل جيتس، المعلوماتية بعد الانترنت، طريق المستقبل، ترجمة عبد السلام رضوان، المجلس الوطني للثقافة والفنون والآداب، العدد 231، الكويت، 1998، ص 41 — 63.

(2) حيث جاء في البند (13) من هذه التوصية على ما يلي :

L'intérêt commun de recueillir، de sauvegarder et de présenter des **preuves électroniques** " **de** manière à garantir au mieux leur caractère irréfutable **.....**"

(3) article 14- Portée d'application des mesures du droit de procédure:".......

C – à la collecte des **preuves électroniques** de toute infraction pénale ...."

(4) المرشد الفدرالي الأمريكي لتفتيش و ضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية "Searching and Seizing COMPUTER and Obtaining Electronic Evidence in Criminal Investigating ": من إعداد قسم جرائم الحاسوب و الملكية الفكرية بوزارة العدل الأمريكية في عام 1994 وصدر له ملحقان في عامي 1997 و199، تحت إشراف أستاذ القانون الجنائي (Orin Kerr) أستاذ بكلية الحقوق في جامعة جورج واشنطن ،تم إعداده بغرض مساعدة سلطات إنفاذ القانون من فهم منطق العالم الرقمي أثناء التحقيقات في جرائم الحاسوب والانترنت ، وأجريت عليه عدة تعديلات ليوافق التطور==

وللدليل الالكتروني ذاتية خاصة يتميّز بها اكتسبها من موضوعه ــ وهي الجريمة الالكترونيّة ــ، وهذه الذاتيّة أثّرت بدورها على إجراءات وطرق الحصول عليه، بحيث لم يعد يعتمد على الإجراءات التقليدية لجمع الدليل الالكتروني(كالمعاينة والتفتيش مثلا) بل تعداه إلى إجراءات حديثة(كالتحفظ المعجل على البيانات المخزنة واعتراض الاتصالات الالكترونيّة الخاصة)، وهو أمر ضروري وفي غاية الأهميّة لمواجهة هذا النوع المستحدث من الجرائم، وذلك لكي نمنع ما يمكن أن يقال من أنّ صعوبة هذا الإثبات قد يؤدي إلى عدم التجريم[1].

وعلى ذلك، سنتناول في هذا الفصل مبحثين، يتعلّق الأوّل بذاتيّة الدليل الالكتروني، والثاني بإجراءات جمع الدليل الالكتروني.

==العلمي في مجال تقنييه المعلومات ، حيث كان آخر تعديل له في يوليو 2002 . ويتكون هذا المرشد من خمسة أبواب:

ــ يتناول **الباب الأول** منه موضوع التفتيش وضبط الأدلة من الحاسوب دون إذن تفتيش، أما **الباب الثاني** فيتناول موضوع التفتيش و ضبط الأدلة بالاستناد إلى إذن. ويتناول **الباب الثالث** موضوع التعامل مع وسائط الاتصالات المقررة في قانون خصوصية الاتصالات . أما **الباب الرابع** فيتناول موضوع المراقبة الالكترونية عبر شبكات الاتصال . أما **الباب** الأخير وهو **الخامس** فيتناول كيفية التحفظ على سجلات الحاسوب كدليل ويناقش موضوعات متعددة كموضوع الأصالة وقاعدة شهادة السماع و أفضل قاعدة للدليل. لمزيد من التفصيل حول هذا المرشد انظر: د/ عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت، المرشد الفدرالي الأمريكي لتفتيش و ضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، بدون دار النشر، 2006 ، ص 9 وما بعدها .

[1] د/ هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، مؤتمر الجمعيّة المصريّة للقانون الجنائي المنعقد بالقاهرة خلال الفترة من (25 إلى 28 أكتوبر 1993)، دار النهضة العربيّة، 1993، ص 576.

المبحث الأوّل
ذاتيّة الدليل الالكتروني

يولد الدليل الجنائي بمولد الجريمة ذاتها، سواء كان ذلك سابقا على ارتكابها في مراحل الترتيب والإعداد أو مرحلة الشروع، أو معاصرا لها عند اقتراف الأفعال الإجرامية، أو لاحقا عند جني ثمارها المؤثمة أو طمس معالمها، فالأدلة بطبيعتها ـ كحقيقة حتمية ـ [1] تتواجد بتواجد الجريمة التي تقع. إذن الدليل الالكتروني يولد أو ينبعث من محله وهي الجريمة الالكترونيّة، أي تلك الواقعة الإجرامية المدعى بحدوثها من قبل سلطات الاتهام، التي يترتب على النجاح في إثبات وقوعها وصحّة إسنادها لفاعليها ثبوت إدانته وتقرير مسؤوليته. ولعل أوّل ما ينبغي علينا القيام به في مستهل هذا المبحث هو تحديد ما المقصود بالجريمة الالكترونيّة وذلك بتعريفها وتحديد خصائصها ثمّ أثر هذه الطبيعة الخاصة على إثباتها جنائيّا وذلك في المطلب الأول، أمّا المطلب الثاني سنتعرض إلى مفهوم الدليل الالكتروني وذلك من خلال تعريفه وبيان الخصائص التي يتميز بها عن غيره من الأدلة التقليديّة وأخيرا أهم تقسيماته.

---

[1] وذلك حسب **نظرية التبادل** " للوكارد"، وتقول هذه النظرية " **أن كل شيء أو أي شخص يدخل مكانا أو مسرحا للجريمة يأخذ معه شيئا و يترك خلفه شيئا منه عند مغادرته** " انظر: د/ خالد حمد محمد الحمادي، الثورة البيولوجية و دورها في الكشف عن الجريمة DNA، دار الجامعة الجديدة، 2005، ص19.

المطلب الأوّل
محل الدليل الالكتروني (الجريمة الالكترونيّة)

قبل الخوض في دراسة الدليل الالكتروني، لابدّ علينا أن نتناول أوّلا محل الدليل الالكتروني، وهي الجريمة الالكترونيّة لأنّه لا يستقيم الحديث عنه إلاّ بعد دراسة هذه الجريمة، والتي تعدّ ظاهرة حديثة نسبيا قياسا بغيرها من الجرائم التقليدية في العالم بشكل أجمع وفي العالم العربي على وجه الخصوص، وربما يرجع السبب في ذلك إلى أنّ أغلب الدول العربية حديثة العهد بتقنيات الحاسوب، كما أنّ الكثير من هذه الدول لم تُدشّن خدمة الانترنت لمواطنيها إلاّ منذ سنوات قليلة فقط .

وعلى ذلك فان الوقوف على أبعاد هذه الظاهرة بشكل كامل يتطلّب منا تعريفها، دراسة خصائصها ومن ثم أثر هذه الطبيعة الخاصة على إثباتها جنائيّا.

الفرع الأوّل
مفهوم الجريمة الالكترونيّة

نشير في البداية إلى أنّه لا يوجد مصطلح قانوني موحد للدلالة على الظاهرة الإجرامية الناشئة في بيئة الكمبيوتر وفيما بعد بيئة الشبكات، بل تباينت هذه المصطلحات حيث رافق هذا التباين مسيرة نشأة وتطور ظاهرة الإجرام المرتبط بتقنية المعلومات فابتداء من اصطلاح إساءة استخدام الكمبيوتر، مرورا بالجرائم المعلوماتية، فجرائم أصحاب الياقات البيضاء إلى جرائم الهاكرز ثمّ جرائم الكمبيوتر والانترنت، ووصولا إلى الجرائم الالكترونية (CyberCrime).

ومهما تكن من تسميات فالمتفق عليه عالمياً ومحلياً هو خطورة تلك الجرائم وتأثيرها السلبي على أمن واستقرار المجتمعات في كلّ الدول المتقدمة والنامية على حد سواء، وكدأب الاكتشافات الجديدة التي تفتح أبواباً وآفاقاً وتدفع بعجلة التقدم والازدهار قدماً من جانب، بينما تفتح أبوابا أخرى للجريمة باختلاف صورها من جانب آخر.

وقد تطرّق **المشرّع الجزائري** على غرار الدول الأخرى مثل فرنسا[1] بتجريم أفعال المساس بأنظمة الحاسب الآلي وذلك نتيجة تأثّر الجزائر بما أفرزته الثورة المعلوماتية من أشكال جديدة من الإجرام التي لم تشهدها البشرية من قبل، ممّا دفع المشرع الجزائري[2]إلى تعديل قانون العقوبات بموجب القانون رقم (04 ــ 15)المؤرخ في العاشر من نوفمبر عام 2004 المتمم للأمر رقم (66 ــ 156) المتضمن قانون العقوبات، والذي أفرد القسم " السابع مكرر" منه تحت عنوان: "**المساس بأنظمة المعالجة الآلية للمعطيات** " والذي تضمن ثمانية مواد (من المادة 394 مكرر وحتى المادة 394 مكرر 7) ونصّ على عدة جرائم هي :

- الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة المعالجة الآلية للمعطيات أو محاولة ذلك (المادة 394 مكرر ف1)، وتضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة (المادة 394 مكرر ف 2).
- الدخول أو البقاء المؤدي إلى تخريب نظام تشغيل المنظومة (المادة 39 مكرر ف 3).
- إدخال أو إزالة أو تعديل ــ بطريق الغش ــ معطيات في نظام المعالجة الآلية (المادة 395 مكرر1).
- تصميم أو بحث أو تجميع أو توفير أو نشر أو الاتجار في معطيات مخزنة أو معالجة أو مراسلة عن طريق منظومة معلوماتية يمكن أن ترتكب بها الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر 2).
- حيازة أو إفشاء أو نشر أو استعمال لأي غرض كان المعطيات المتحصل عليها من إحدى الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر2).

وقد ضاعف المشرع العقوبات المنصوص عليها في هذا القسم إذا استهدفت الجريمة الدفاع الوطني أو الهيئات و المؤسسات العمومية (المادة 394مكرر3)، وتجدر

---

(1) في سنة 1994 تمّ تعديل قانون العقوبات الفرنسي حيث تمّ إضافة فصلا ثالثا للباب الثاني من القسم الثالث من قانون العقوبات، و سمي هذا الفصل " الاعتداءات على نظم المعالجة الآلية للمعطيات " " Des atteintes aux systèmes de traitement automatisé de données "، وجاء من المادة (1/323 إلى المادة 323 /7). انظر في التطور التشريعي للجريمة المعلوماتية في القانون الفرنسي: د/ أحمد حسام طه، الجرائم الناشئة عن استخدام الحاسب الآلي، المرجع السابق، ص 82 .

(2) جاء في عرض أسباب هذا التعديل " **أن التقدم التكنولوجي و انتشار وسائل الاتصال الحديثة أدى إلى بروز إشكال جديدة للإجرام مما دفع بالكثير من الدول إلى النص على معاقبتها، وانّ الجزائر على غرار هذه الدول تسعى من خلال هذا المشروع إلى توفير حماية جزائية للأنظمة المعلوماتية وأساليب المعالجة الآلية للمعطيات، وانّ هذه التعديلات من شانها سد الفراغ القانوني في بعض المجالات، وسوف يمكّن لا محالة من مواجهة بعض أشكال الإجرام الجديد** ".

الإشارة إلى ان المشرع الجزائري اتبع نفس نهج المشرع الفرنسي من خلال إقراره لمسؤولية الشخص المعنوي بموجب المواد (18مكرر ،18مكرر1) من القانون رقم (04ـــ15)، وشدّدت عقوبة الغرامة علي الشخص المعنوي إلي خمس مرات للحدّ الأقصى المقرر للشخص الطبيعي (المادة 394 مكرر4).

كما عاقبت تلك المواد على الاشتراك في مجموعة أو في اتفاق يتألّف بغرض الإعداد لجريمة أو أكثر من الجرائم المنصوص عليها في هذا القسم (المادة 394 مكرر5).

ونصّ هذا التعديل على عقوبة مصادرة وسائل ارتكاب الجريمة - الأجهزة والبرامج- وإغلاق المواقع التي تكون محلاّ لها، علاوة على إغلاق المحل أو المكان الذي ارتكبت فيه الجريمة (المادة 394 مكرر7).

وفي عام 2006 أدخل تعديل آخر على قانون العقوبات الجزائري بموجب القانون رقم (06 ـــ 23) المؤرخ في 20 ديسمبر سنة 2006، حيث مسّ ذلك التعديل القسم السابع المكرر والخاص **بالجرائم الماسة بأنظمة المعالجة الآلية للمعطيات**، وقد تمّ تشديد عقوبة الحبس والغرامة [1] المقررة لهذه الأفعال فقط دون المساس بالنصوص التجريمية الواردة في هذا القسم (القسم السابع مكرر) من القانون رقم (04ـــ15)، وربما يرجع سبب هذا التعديل إلى ازدياد الوعي بخطورة هذا النوع المستحدث من الإجرام باعتباره يؤثر على الاقتصاد الوطني بالدرجة الأولى وشيوع ارتكابه ليس فقط من الطبقة المثقفة بل من قبل الجميع بمختلف الأعمار ومستويات التعليم نتيجة تبسيط وسائل تكنولوجيا المعلومات وانتشار الانترنت كوسيلة نقل المعلومات حيث ازداد معدل استعمال الانترنت في المجتمع الجزائري: 4.120.0% من سنة2000 إلى 2007 [2].

---

[1] مثال ذلك : يّعاقب على الدخول أو البقاء عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية بالحبس من ثلاث (3)أشهر إلى سنة (1)سنة و بغرامة مالية من 50000دج إلى 200000دج طبقا للقانون رقم (06ـــ 23) بينما كانت العقوبة على نفس الجريمة في القانون القديم هي الحبس من ثلاث (3) أشهر إلى(1) سنة وغرامة من 50000دج إلى 100000دج.

[2] عدد مستخدمي الانترنت في المجتمع الجزائري سنة 2000 حوالي(50الف) مستخدم ، وصل سنة 2007 إلى (246000) مستخدم .

أما في المجتمع المصري كان 45الف مستخدم ووصل في 2007 إلى 6 مليون مستخدم أي ارتفع بمعدل 1.233.3%. هذه الإحصائيات ماخوذة من الموقع التالي:

http://www.stratime2.com/asp?=6565821

وانظر أيضا المؤتمر القومي الأول لتطوير منظومة البحث العلمي ،المنعقد في مايو 2005، تحت رعاية السيد الرئيس محمد حسني مبارك.

وانطلاقا ممّا سبق ذكره نلاحظ أنّ المشرّع الجزائري استخدم مصطلح **المساس بأنظمة المعالجة الآلية للمعطيات**، وهو في نظرنا مصطلح غير دقيق لأنّه يقتصر فقط على جرائم الكمبيوتر دون الانترنت وإن كانت الأفعال التي نصّ بتجريمها تشمل في نفس الوقت جرائم الانترنت.

وعلىّ ذلك نفضل من جانبنا استخدام مصطلح **الجريمة الالكترونية** في دراستنا هذه ويرجع ذلك للأسباب التالية:

1ـ إن المصطلحات القانونية لابّد وأن تتّصف بالمرونة وبعد النظر، فهذه الجريمة ناشئة أساسا من التقدم التكنولوجي ومدى التطور الذي يطرأ عليها وهو متجدّد بصفة دائمة خاصة في مجال تكنولوجيا المعلومات والاختراعات الالكترونية وغيرها من الأجهزة التقنية التي قد تظهر في المستقبل .

ولعلّ ما يدلّ على ذلك أنّ وحدة مكافحة الجرائم الالكترونية في شرطة نيوزلندا استخدمت في تعريفها للجريمة الالكترونية " **الهاتف المحمول" Mobile phone** " سواء كان أداء للجريمة أو هدفا لها [1].

2ـ مصطلح الجريمة الالكترونية اصطلاح شامل لكل من جرائم الحاسوب والانترنت وغيرها من الجرائم الناتجة عن استخدام الشبكات المحلية للاتصال، ويشمل في مضمونه الجرائم التي تستهدف النظم المعلوماتية والشبكات كهدف فضلا عن الجرائم التي تستخدم الكمبيوتر وهذه الشبكات كوسيلة لارتكاب جرائم أخرى.

وعلى ذلك سنتناول فيما يلي بيان أهمّ التعاريف التي قيلت بشأن الجريمة الالكترونية(أوّلا)، مرورا بتحديد خصائصها(ثانيا)، وأخيرا مدى صعوبة اكتشاف واثبات الجريمة الالكترونيّة باعتباره من أهمّ أثار الطبيعة الخاصة بهذا النوع المستحدث من الإجرام.

---

[1] محمد بن نصير محمد السرحاني، مهارات التحقيق الفني في جرائم الحاسوب والانترنت، دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية في العلوم الشرطية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2004، ص29.

يتشابه الهاتف الخلوي إلى حد كبير مع إمكانيات الكمبيوتر، مثل الرسائل الالكترونية والصور عن طريق تقنية البلوثوث، أيضا الدخول إلى الانترنت فهو تقنية من تقنيات الحوسبة المتطورة ، لذلك يرى البعض انه من غير المعقول إخضاعها إلى قانون الاتصالات، نظرا للمخاطر التي تنجم عنه .انظر: د/ فايز الظفيري، الأحكام العامة للجريمة الالكترونية، مجلة العلوم القانونية والاقتصادية، العدد الثاني، السنة الرابعة والأربعون، يوليو 2002 ، ص 489 ـ 490 .

أوّلا: تعريف الجريمة الالكترونيّة: تعدّ مسالة تعريف جرائم الكمبيوتر والانترنت هذه هي الأخرى من المسائل الشائكة التي تقف حجر عائق أمام رجال القانون حيث يصعب حتى الآن وضع تعريف عام وشامل لهذه الجرائم، وقد أثار ذلك العديد من المشاكل العملية تتمثل أهمها في: ــ صعوبة تقدير حجم الظاهرة ، ــ تعذر إيجاد الحلول اللازمة لمواجهتها، ــ كذلك صعوبة تحقيق التعاون الدولي لمكافحتها [1] .

وقد عرّف البعض[2] الجريمة المعلوماتية بأنّها" **فعل إجرامي يستخدم الحاسب في ارتكابه كأداة رئيسية** "[3]. أمّا خبراء منظمة التعاون الاقتصادي والتنمية (OECD) عرفوها بأنها:"**كل سلوك غير مشروع أو غير أخلاقي أو غير مصرح به يتعلّق بالمعالجة الآلية للبيانات و/أو نقلها**"[4]. أمّا البعض الآخر[5] فقد عرفها بأنها "**أية جريمة يكون متطلبا لاقترافها أن تتوافر لدى فاعلها معرفة بتقنية الحاسبات** ".

كما حاول البعض تحديد المقصود من جرائم الانترنت :حيث عرفها بأنها:"**مجموعة الجرائم الجنائية التّي ترتكب عبر شبكة الانترنت**"[6]، أو هي" **تلك الجرائم التي لا تعرف الحدود الجغرافية، والتي يتمّ ارتكابها بأداة هي الحاسب الآلي، عن طريق شبكة الانترنت، وبواسطة شخص على دراية فائقة بها** "[7]، كما تعرف بأنها " **مجموعة الأفعال والأعمال غير القانونيّة التي تتمّ عبر شبكة الانترنت أو تبثّ عبر محتوياتها**"[8].

---

[1] د/ نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصاديّة، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقيّة، 2005، ص 28.

[2] مثل الأستاذ (Leslie D.Ball) ، انظر: د/ هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، السنة الرابعة ،العدد الثاني، يوليو 1999 ، 78.

[3] د/ هشام محمد فريد رستم، الجرائم المعلوماتية، نفس المرجع، ص 78 .

[4] انظر موقع المنظمة على شبكة الانترنت :

www.oecd.org

[5] (David Thompson) في مؤلفه:

David Thompson , Current Trends in Cimputer Crime, Computer Control Quarterly, vol .9, no 1, 1991,p.2.

[6] La cybercriminalité:" c'est l'ensemble des infraction pénale qui se commettent sur le réseau internet" La définition du ministre de l'intérieur français, disponible en ligne à l'adresse suivant:

.Free.fr http:// vsabourni

[7] منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت، دار الفكر الجامعي، الإسكندرية، 2004، ص 13.

[8] د/ عادل عبد الجواد محمد، إجرام الانترنت، مجلة الأمن والحياة، أكاديمية نايف العربيّة للعلوم الأمنيّة، العدد 221، السنة العشرون، ديسمبر 2000ــ يناير 2001، ص 70.

بالنظر إلى جملة التعريفات السابقة، نلاحظ أنها تتّسم في بعض الحالات بنوع من الشمولية المطلوبة، فليس بمجرد اشتراك الحاسب الآلي أو شبكة المعلومات في الجريمة نصبغ عليها وصف جرائم الكمبيوتر أو الانترنت، ذلك أنه يمكن أن تستهدف بعض الجرائم الكيانات المادية والأجهزة التقنية كسرقة الحاسب أو تخريب الشبكات وهي محل صالح لتطبيق نصوص التجريم التقليدية، لأنّ الاعتداء فيها يقع على مال مادي منقول، عكس الجرائم التي تطاول الكيانات المنطقية من برامج ومعطيات، مما تثير إشكالية انطباق النصوص الجنائية التقليدية عليها .

وفي مقابل ذلك نلاحظ أن هناك بعض التعريفات[1] تضيق من هذه الجرائم حيث يشترط في الفاعل دراية عالية بتقنية المعلومات وهو ما لا يتحقق، في كثير منها ، لأنّ تبسيط وسائل المعالجة و تحويل الأجهزة المعقدة فيما سبق إلى أجهزة سهلة الاستخدام مكّنت الفاعل ارتكاب جريمته دون معرفة كبيرة بالمعلوماتية، فإرسال رسالة تحمل فيروسا إلى شخص ما لا يتطلب إلاّ معرفة محدودة من هذه التقنية .

فضلا عن ذلك، نلاحظ أنّ هذه التعريفات وضعت حدودا فاصلة بين جرائم الكمبيوتر والانترنت، ممّا أدى إلى التمييز بين الأفعال التي تستهدف المعلومات في نظام الكمبيوتر ذاته خلال مرحلة المعالجة، والتخزين، والاسترجاع (جرائم الكمبيوتر)[2]، وبين الأفعال التي تستهدف الشبكات ذاتها أو المعلومات المنقولة عبرها (جرائم الانترنت)، فهذا التمييز غير دقيق بل مخالف للمفاهيم التقنية وللمراحل التي توصّل إليها تطوّر وسائل تقنية المعلومات في الدمج بين وسائل الحوسبة والاتصال، فهناك مفهوم عام لنظام الكمبيوتر حيث يستوعب كافة المكوّنات المادية والمعنوية المتصلة بعمليات الإدخال والمعالجة والتخزين والتبادل (أي نقل هذه المعلومات عبر الشبكات)، ممّا يجعل الشبكات وارتباط الكمبيوتر بالانترنت من فكرة واحدة وهي تكاملية النظام .

والملاحظ أنّ المشرع الفرنسي يتبنّى هذا الموقف، ويظهر ذلك من خلال نص المادة (321 ــ1) من قانون العقوبات الفرنسي الجديد، حيث تجرّم هذه المادة فعل الدخول أو البقاء

---

[1] مثل: تعريف الأستاذ (David Thompson)

[2] جميع جرائم الكمبيوتر يمكن أن ترتكب داخل شبكة المعلومات بل انه لم يظهر البعد الحقيقي لها إلاّ بعد ارتكابها عن طريق هذه الشبكات مثل جرائم القرصنة . انظر: د / نائلة عادل محمد فريد قورة، المرجع السابق، ص35. في نفس المعنى، انظر: علي أحمد الفرجاني، جريمة القرصنة المعلوماتية ــ دراسة مقارنة من الجانبين الموضوعي والإجرائي ــ مجلة التشريع، السنة الثانية، العدد السابع، أكتوبر 2005 ، ص 17. وانظر أيضا: أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، إسكندرية، 2008، ص 105.

غير المشروع داخل نظم المعالجة الآلية للمعطيات، وقد أجمع الفقه الفرنسي من واقع الأعمال التحضيرية للقانون أن نظام المعالجة الآلية للمعطيات ينصرف إلى المعلومات والنظام الذي يحتوي عليها، وكذلك إلى شبكات المعلومات، حيث أحالت المناقشات السابقة على تبنّي القانون في تعريف نظم المعالجة الآلية للمعطيات إلى التعريف الوارد لها في القانون الصادر عام (1978)، والخاص بالمعلوماتية وحماية الحريات [1]، ويشمل وفق هذا القانون جميع العمليات التي تتمّ بواسطة الوسائل الالكترونية، من جمع وتخزين ومعالجة وحفظ ونقل المعلومات، ونشير إلى أنّ المشرع الجزائري أخد كذلك بهذا الاتجاه، ويبدو ذلك واضحا من خلال المادة (394 مكرر) من قانون العقوبات الجزائري [2] من القانون رقم(04 ـــ 15)المؤرخ في العاشر من نوفمبر عام 2004 م، هذا من جهة .

ومن جهة أخرى تتطلب أنشطة الانترنت أجهزة كمبيوتر ترتكب بواسطتها وهي تستهدف أيضا معلومات مخزنة أو معالجة ضمن أجهزة كمبيوتر هي **الخوادم** التي تستضيف مواقع الانترنت أو تديرها [3]. وإذا أردنا فصل وسائل تقنية المعلومات، فانّ هذا لن يتحقق لأنّ الشبكات ذاتها عبارة عن برمجيات و بروتوكولات مدمجة في نظام الحوسبة ذاته، إلاّ أذا أردنا أن نحصر فكرة الشبكات بالأسلاك وهذا يخرجنا من نطاق جرائم الكمبيوتر والانترنت إلى جرائم الاتصالات التي تستهدف ماديات الشبكة .

بناء على ذلك، عرف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا عام 2000، الجريمة الالكترونية بأنها" **أيّة جريمة يمكن ارتكابها بواسطة**

---

[1] د/ أمين أعزان، الحماية الجنائية للتجارة الالكترونية، رسالة دكتورا، كلية الحقوق، جامعة عين شمس، 2007، ص 131 وما بعدها.

[2] تنص المادة (394 مكرر) " يعاقب بالحبس من ثلاث (3) أشهر السنة (1) وبغرامة مالية من 50،000دج إلى 200،000 دج كل من يدخل أو يبقى عن طريق الغش في كل أو جزء من منظومة للمعالجة الآلية للمعطيات أو يحاول ذلك.

تضاعف العقوبة إذا ترتب على ذلك حذف أو تغيير لمعطيات المنظومة .

وإذا ترتب على الأفعال المذكورة أعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة (6) أشهر إلى سنتين (2) والغرامة من 50،000 دج إلى 300،000 دج ."

[3] يونس عرب ،جرائم الكمبيوتر والانترنت ،المعنى والخصائص والصور وإستراتيجية المواجهة القانونية،على الموقع التالي :

Arablaw.org/download/cybercrimes_-general.doc .www

نظام حاسوبي،أو شبكة حاسوبية أو داخل نظام حاسوب ،وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية" [1].

ونحن من جانبنا نتفق مع هذا التعريف لأنّه حاول الإحاطة قدر الإمكان بجميع الأشكال الإجرامية للجريمة الالكترونية سواء التي تقع بواسطة النظام المعلوماتي ـــ المزواج بين تقنيات الحوسبة والاتصال، بما في ذلك شبكة المعلومات ـــ أو داخل هذا النظام على المعطيات والبرامج، كما تشمل جميع الجرائم التّي من الممكن أن تقع في البيئة الالكترونية، فلم يركّز على فاعل الجريمة ومقدرته التقنية، ولا على وسيلة ارتكاب الجريمة، بل حاول عدم حصر هذه الجريمة في نطاق ضيّق يتيح المجال أمام إفلات العديد من صور هذه الجريمة من دائرة التجريم.

وتجدر الإشارة في هذا المقام أنّه أكثر الجرائم الالكترونية التي يتمّ ارتكابها يكون الهدف الأساسي منها الحصول على المعلومات الالكترونية بما تشمله من بيانات ومعطيات، بالإضافة إلى البرامج بكافة أنواعها والتّي تكون إمّا مخزنة في أجهزة الحاسوب أو تلك المنقولة عبر شبكة الانترنت، إلاّ أن هذه المعلومات لم تُعد الهدف الوحيد للمجرم الالكتروني بل تعدّته لتطال الاعتداء على الأشخاص والأموال .

ومن أمثلة جرائم الاعتداء على الأشخاص **ـــ جرائم الأخلاق** كالقذف والسب والتشهير عبر الانترنت وغيرها من وسائل الاتصال الحديثة كالهاتف المحمول عن طريق تقنية الرسائل سواء كانت الرسائل نصية أو عن طريق وسائط(SMS. MMS). وكذلك **جرائم الاستغلال الجنسي للأطفال** حيث أصبحت شبكة الانترنت تمثل فضاء لصناعة ونشر صور ومواقع الإباحية الجنسية وجعلها متاحة للجميع، بحيث ارتفع عدد المواقع الإباحية لاستغلال الأطفال بنسبة (400%) بين سنة 2004 و 2005 .

فضلا عن ذلك، جرائم **الاعتداء على حرمة الحياة الخاصة** :سواء حرمة البيانات الشخصية المخزنة في قواعد ونظم المعلومات كالدخول والتداول غير المرخص به للمعلومات واستخدام هذه البيانات لغير الغرض الذي أعدت من اجله، أو حرمة الإنسان في المراسلات والأحاديث الخاصة كالتصنت والاطلاع عليها واعتراضها .

أمّا بالنسبة للجرائم المالية، فقد أصبح الحاسوب يمثل أداة سلبية للاعتداء على أموال الغير لاسيما في نطاق شبكة الانترنت، ممّا أدى إلى خلق صور مستحدثة من الجرائم كجريمة غسل

---

[1] مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين الذي انعقد في فينا في الفترة ما بين (10ـــ 17) نيسان لعام 2000، مشار إليه عند: د/ أسامة أحمد المناعسة، جلال محمد الزغبي وفاضل الهواوشة، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان، الطبعة الأولى، 2001، ص78.

الأموال عبر الانترنت [1]، والجرائم المتعلقة بالتجارة الالكترونية كالتعامل في البيانات بدون ترخيص، أو التصريح عمدا بمعطيات خاطئة، وجريمة التهريب الضريبي ..[2]، أيضا جرائم السطو على أرقام البطاقات الائتمانية(النقود الالكترونية)[3].

ثانيّا: **خصائص الجريمة الالكترونيّة**

إنّ ارتباط الجرائم الالكترونية بجهاز الحاسوب وشبكة الانترنت أضفى عليها مجموعة من الخصائص المميزة لها عن باقي الجرائم التقليدية، سواء تعلقت هذه الخصائص بطبيعة المحل الذي يقع عليها الاعتداء أو بالشخص مقترف هذه الجرائم أو بأسلوب ارتكابها، أو تعلّق الأمر بالنطاق المكاني للجريمة وذلك ما سنتناوله في التالي:

أ ـ طبيعة محل الاعتداء: من المعروف أنّ الاعتداء قد يقع على الأموال كما يقع على الأشخاص وفي كلا الحالتين يتمتّع بطبيعة خاصة في البيئة الالكترونيّة، وذلك على النحو التالي:

بالنسبة **للمال محل الاعتداء:** فقد أصبحت المعلومات بما تشمله من معطيات وبرامج الهدف الرئيسي لمرتكبي الجرائم الالكترونية، وذلك نتيجة للقيمة الاقتصادية العاليّة التّي تمثلها

---

[1] ظهر اصطلاح (غسل الأموال) لأول مرة في اتفاقية الأمم المتحدة لمكافحة الاتجار غير المشروع في المخدرات والتي عقدت في فينا عام 1998، وقد نصت في المادة الثالثة منها على أن غسل الأموال يتمثّل أمّا في تحويل الأموال، أو نقلها مع العلم بأنها من نتاج المخدرات، أو في إخفاء أو تمويه حقيقة والأموال أو مصدرها أو في اكتساب أو حيازة أو استخدام الأموال مع العلم وقت تسليمها أنها من حصيلة جريمة من الجرائم المنصوص عليها في الاتفاقية .

ــ فغسل الأموال بصفة عامة هو معالجة لمصدر الدخل الأول غير المشروع (الناجم عن جريمة) بالقيام بمجموعة تحركات اقتصادية مشروعة تؤدي إلى طبع الأموال غير مشروعة المصدر بطابع المشروعية== == وبطريقة لا يمكن بمقتضاها التعرف على المصدر الأصلي (غير المشروع). انظر: د/ عمر بن يوسف ود/ يوسف أمين شاكير،غسل الأموال عبر الانترنت، ط1، أقاسوس، القاهرة ،2004، ص 31 . كذلك: عبد الفتاح سليمان، مكافحة غسيل الأموال، دار علاء الدين، القاهرة، الطبعة الأولى، 2004، ص 8 وما بعدها . وانظر أيضا: محمد علي العريان، عمليات غسل الأموال وآليات مكافحتها ــ دراسة مقارنة ــ دار الجامعة الجديدة للنشر، الإسكندرية، 2005 ص 27 وما بعدها .

[2] د/ هدى حامد قشقوش، الحماية الجنائيّة للتجارة الالكترونيّة، دار النهضة العربيّة، القاهرة، ص 36 وما بعدها

[3] أثبتت شبكة (MSNBC) عمليا مدى سهولة الحصول على أرقام البطاقات الائتمانية من شبكة الانترنت حيث قامت بعرض قوائم تحتوي على أكثر من 2500 رقم بطاقة ائتمانية حصلت عليها من سبع مواقع للتجارة الالكترونية، وذلك عن طريق استخدام قواعد بيانات متوافرا تجاريا، حيث يستطيع أي متطفل الحصول عليها، واستخدامها في عمليات شراء يدفع الثمن فيها أصحاب البطاقات الحقيقيون. وهو ما أكّده مساعد وزير الداخلية المصري للمعلومات حين صرّح بان جرائم الاستخدام غير الشرعي لبطاقات الائتمان الالكترونية تكلف حوالي ثلاث (3) ملايين جنيه سنويا.

قد تفوق قيمة الأموال المادية[1]، إلاّ أنّ طبيعة هذه الأموال في حالتها المجردة من الوسائط المادية تثير عدّة مشاكل في تحديد موضوع الجريمة من جهة، ومدى انطباق القوانين الجنائية التقليدية عليها من جهة أخرى، باعتبارها مجرد نبضات الكترونية غير مرئية في فضاء تخيلي وليست ذات كيان مادي مما أدّى إلى خلق اتجاهات متباينة في تحديد الطبيعة القانونية للمعلومات، فمنهم من أنكر عنها صفة المال والبعض الآخر أصبغ عليها وصف المال نظرا لقابليتها للحيازة والتملك، وهناك اتجاه ثالث اعتبرها أموالا ذات طبيعة خاصة وذلك في الفقه الفرنسي الجديد[2]. إلاّ أنّه ينبغي على التشريعات التدخل لحلّ هذه المشكلة بتشريع خاص حماية لهذه المعلومات، يبين فيه الطبيعة القانونية لها ويجرّم فيه مختلف صور العدوان الواقعة عليها، لاسيما وأن نظام العقاب الجزائي محكوم بقاعدتين هما: مبدأ الشرعية الموجب لعدم إمكان العقاب على أيّ فعل دون نص، وقاعدة حظر القياس في النصوص التجريمية الموضوعية.

أمّا طبيعة شخص المجني عليه في الجريمة الالكترونية: غالبا ما يستهدف المجرم الالكتروني أشخاصا اعتبارية متمثلة في مؤسسات مالية حيث بلغت نسبة الجريمة فيها (19%) من مجموع الجرائم المرتكبة، كما تستهدف أيضا المؤسسات العسكرية، كالتجسس العسكري عن طريق الشبكات من خلال الأقمار الصناعية [3]، كما يمكن أن يكون الاعتداء واقعا على أشخاص طبيعية كما هو الحال بالنسبة لجرائم القذف والتشهير، كذلك جرائم النصب عبر

---

[1] يقول القاضي الفرنسي (لويس جوانيه Louis Joinet) في هذا المعنى أنّ " المعلومات قوة اقتصادية، والقدرة على تخزين أنواع معينة من البيانات ومعالجتها يمكن أن يعطي بلدا مميزات أساسية وتكنولوجية على البلدان الأخرى، وهو ما قد يؤدي إلى فقدان السيادة الوطنية لتلك البلدان من خلال انتقال البيانات فيما بين الدول" مشار إليه عند: د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992، ص 16 .

[2] يعتبر هذا الاتجاه أن المعلومات أموالا ذات طبيعة خاصة نتيجة غياب الكيان المادي لها ممّا لا يجعلها محلا لحق مالي من الحقوق المتعارف عليها في الفقه والتي ترد على كيانات مادية، لذلك يلزم بالضرورة استبعادها من طائفة الأموال، ولا يقصد بهذا الاستبعاد أن تضل المعلومات عارية من أيّ حماية في حالة الاعتداء عليها، لان هذا الأخير يعد خطأ يحرك مسؤولية فاعله، والسائد لدى جانب من الفقه الفرنسي أنّ هذه المسؤولية تتحرك وفق قواعد المسؤولية المدنية المستندة إلى نص المادة (1382) من القانون المدني الفرنسي . انظر: د/ عبد العظيم وزير، شرح قانون العقوبات ــ القسم الخاص ــ جرائم الاعتداء على الأموال، الطبعة الأولى، دار النهضة العربية، القاهرة، 1993، ص 40.

[3] اتجهت فرنسا إلى إطلاق أربعة أقمار صناعية من اجل فك رموز وشفرات، وتسجيل كافة المكالمات التلفونية والفاكسات والبريد الالكتروني في جميع إنحاء العالم، وتمّ تشغيل هذا النظام سنة 2003 تحت اسم (سرب النحل) مما جعل فرنسا ثالث دولة بعد الولايات المتحدة الأمريكية و روسيا في التجسس. انظر: د/ أيمن عبد الحفيظ عبد الحميد سليمان، إستراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، أكاديميّة الشرطة، ص 231.

الشبكات، حيث وقع الشعب الأمريكي ضحية هذا الإجرام من قبل بعض الأشخاص مستغلين في ذلك أحداث (11 سبتمبر 2001)، نتيجة قيام العديد من الجهات بإنشاء مواقع على شبكة الانترنت بغرض جمع تبرعات لضحايا الحادث.

ب ـ خصوصية مجرمي المعلوماتية: يتّسم المجرم المعلوماتي بخصائص معيّنة تميّزه عن المجرم في الجرائم التقليدية، وذلك في عدة جوانب:

1 ــ <u>من حيث سمات شخصية المجرم المعلوماتي</u> : حيث تقترب في كثير من الأحيان من سمات المجرمين ذوي الياقات البيضاء، فكلاهما قد يكونوا من ذوي المناصب الرّفيعة المستوى، ويتمتعون بالاحترام والثقة العاليين ولهم القدرة على التكيف الاجتماعي، فضلا عن ذلك يمتلك هذا المجرم المعلوماتي المهارة والمعرفة في استخدام التقنية المعلوماتية وهذه المهارة إمّا اكتسبها عن طريق الدراسة المتخصصة في هذا المجال أو بالخبرة والاحتكاك بالآخرين، كما يتميّز هذا المجرم بالذكاء، حيث أنّ الجريمة الالكترونية تتطلب مقدرة عقلية وذهنية خاصة في الجرائم الماليّة.

2 ــ <u>من حيث الدافع إلى ارتكاب الجريمة</u>: تتباين دوافع ارتكاب الجريمة الالكترونية تبعا لطبيعة المجرم ومدى خبرته في مجال الحاسب الآلي، وهي عادة تدور بين تحقيق الكسب المادي، كالمساومة على البرامج أو المعلومات المتحصّلة بطريق الغش مثلا [1]، وقد تكون المتعة والتحدي والرغبة في قهر هذا النظام المعلوماتي واثبات الذات، أو الرغبة في الانتقام من رب العمل[2]، كما يعدّ التسابق الفضائي والعسكري دافعا لهذه الجريمة، حيث قام القراصنة بالإغارة على شبكات معلوماتية تابعة لوكالة الفضاء ناسا ومواقع أسلحة ذرية تابعة لحكومة الولايات المتحدة الأمريكية [3].

---

(1) لقد أثارت مجلة (Security Inform Atiqne) وهي مجلة متخصصة في الأمن المعلوماتي، أنّ (43%) من حالات الغش المعلن عنها قد تمت من اجل اختلاس أموال و(23%) من أجل سرقة معلومات و(19%) أفعال إتلاف، و(15%) سرقة وقت الآلة . مشار إليه عند أمين الرومي، جرائم الكمبيوتر والأموال، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003، ص 24 .

(2) قام أحد المسئولين الاعلاميين بإحدى الشركات بعد فصله عن العمل بزرع قنبلة منطقية زمنية في برنامج لمدة شهر كامل مما كبد الشركة خسائر كبيرة . انظر زكي محمد الوطنان ، جرائم الحاسب الآلي ، دراسة نفسية تحليلية ، مقال موجود على الموقع التالي :.

. http://www.minshawi.com.PDR other/oteyom.

(3) كان من جراء ذلك أن قام البنتاجون بإنشاء "مركز الحرب المعلوماتية " للدفاع عن الولايات المتحدة الأمريكية ضد القراصنة . مشار إليه عند : د/ هلالي عبد الله أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001 ، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003 ، ص 21 ــ 22 .

3 ـ **من حيث أنماط مجرمي المعلوماتية** : يمكن تصنيف مرتكبي الجرائم الالكترونية على أساس أغراض الاعتداء إلى الفئات التالية: الفئة الأولى، المخترقون وتضم نوعين من المتطفلين الهاكرز (Hackers) والكراكز (Crackers) [1]، أما الفئة الثانية فتشمل المحترفين، وتعد الأخطر من بين مجرمي التقنية حيث تهدف اعتداءاتهم أساسا إلى تحقيق الكسب المادي، أو تحقيق أغراض سياسية. أمّا فئة الحاقدين لا يسعون إلى إثبات قدراتهم الفنية ولا إلى مكاسب مادية فما يحرك نشاطهم سوى الرغبة بالانتقام والثأر من رب العمل[2]. وهناك طائفة ظهرت حديثا هي فئة صغار نوابغ المعلوماتية أو (المتلعثمين) [3]، ويرى جانب من الفقه الجنائي بشأنهم أنه من غير الملائم تصنيف هؤلاء الشباب ضمن الطوائف الإجرامية لان لديهم ببساطة ميلا للمغامرة والتحدي و الرغبة في الاكتشاف [4].

ج ـ أسلوب ارتكاب الجريمة الالكترونية: الطبيعة الخاصة بالجريمة الالكترونية تبرز بصورة واضحة في أسلوب ارتكابها، فإذا كانت بعض الجرائم التقليدية تتطلب نوعا من المجهود العضلي الذي يكون في صورة ممارسة العنف والإيذاء كما هو في جريمة القتل أو الاختطاف مثلا، فالجرائم الالكترونية هي جرائم هادئة، كلّ ما تتطلبه عدد من اللمسات على أزرار لوحة المفاتيح حتّى تؤدي إلى إسقاط الحواجز الأمنية للنظم والشبكات، حيث تحتاج إلى قدرة علمية

---

(1) **الهكرة** : نظرا لعدم وجود ترجمة لها باللغة العربية، فتستخدم الكلمة كما هي باللغة الانجليزية " Hackers " وهم متطفلون يتحدون إجراءات أمن النظم و الشبكات ، لكن لا تتوافر لديهم في الغالب دوافع حاقدة أو تخريبية ، وإنما ينطلقون من دوافع التحدي و إثبات الذات، وتتألف هذه الطائفة أساسا من مراهقين وشباب . أما **الكراكر**: هم أشخاص يقومون بالتسلل إلى نظم الحاسوب للاطلاع على المعلومات المخزنة فيها لإلحاق الضرر أو العبث بها أو سرقتها وذلك بدافع التحدي الإبداعي، وتتراوح أعمارهم مابين (25 ـ 40 عام). انظر: د/ مصطفى محمد موسى ، أساليب إجرامية بالتقنية الرقمية ماهيتها. مكافحتها ، دراسة مقارنة ، مطابع الشرطة ، الطبعة الأولى ، 1423 هـ ـ 2003 م ، ص 15 وما بعدها.

(2) أجرى مركز الدراسات الاجتماعية والاقتصادية بفرنسا CESE دراسة عام 1988، تبن أن حوالي (65%) من الجرائم محل الدراسة ارتكبها عاملون في المؤسسة المجني عليها وكانت النسبة(85%) في دراسة أخرى أجرتها اللجنة المحاسبية بالمملكة المتحدة دامت عام 1993. مشار إليه عند: د/ نائلة قورة، المرجع السابق، ص 82 .

(3) للتدليل على خطورة أفعال هذه الفئة، نذكر على سبيل المثال تلاميذ المدرسة الثانوية في ولاية مانهاتن الذين استخدموا عام 1980 طرفيات غرف الدرس للدخول إلى شبكة الاتصالات ودمروا ملفات زبائن الشركة في هذه العملية. انظر: د/ عبد الفتاح بيومي حجازي، الأحداث والانترنت، دار الفكر الجامعي ، الإسكندرية، 2004، ص 56 . ولمزيد من التفصيل حول مختلف أنماط وفئات المجرم المعلوماتي، انظر: د/ أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، أكاديمية الشرطة، ص 211 وما بعدها. وانظر أيضا: د/ نائلة عادل محمد فريد قورة، المرجع السابق، ص 61 وما بعدها. وانظر كذلك: د/ عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية ،القاهرة، 2002، ص 52 وما بعدها .

(4) د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998، ص40.

في مجال التعامل مع جهاز الحاسوب وشبكة المعلومات الدولية " الانترنت "[1]، بما في ذلك بعض تقنيات ارتكاب هذه الجرائم كالاختراق سواء عن طريق استعمال نظم التشغيل أو باستخدام البرامج أو عن طريق تشمّم كلمات السر وجمعها [2]، كما ظهرت تقنيات السلامي (Salami Technique) [3] أو حصان طروادة (Trojan Horse) [4] في ارتكاب عملية الاختلاس المالي، وغيرها من الأساليب المتطورة التي أفرزتها التكنولوجيا.

د ـ الجريمة الالكترونية متعدية الحدود أو جريمة عابرة للحدود: المجتمع المعلوماتي لا يعترف بالحدود الجغرافية، فهو مجتمع منفتح عبر شبكات تخترق الزمان والمكان، دون أن تخضع لحرس الحدود، خاصة بعد ظهور شبكات المعلومات الدولية "الانترنت "حيث يمكن نقل كم هائل من المعلومات بين عدة أنظمة يفصل بينها آلاف الأميال، كل ذلك أدّى إلى نتيجة مؤداها تأثر عدّة دول بالجريمة الالكترونية الواحدة في آن واحد، حيث يمكن أن تقع الجريمة من جان في دولة على مجني عليه في دولة أخرى في وقت يسير جدا مكبدة أفدح الخسائر. فهذه الطبيعة التي تتميز بها الجريمة الالكترونية أدت إلى خلق العديد من المشاكل حول تحديد الدولة صاحبة الاختصاص القضائي بهذه الجريمة، وكذلك حول القانون الواجب تطبيقه، بالإضافة إلى إشكاليات تتعلق بإجراءات الملاحقة القضائية، وغيرها من المشاكل التي تثيرها الجرائم العابرة للحدود بشكل عام [5]. لذلك فان عولمة الجريمة بهذا المعنى تقتضي عولمة

---

[1] د/ محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع، 2004، ص 165. كذلك نهلا عبد القادر المومني، الجرائم المعلوماتيّة، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2008، ص 47 . وانظر أيضا: د/ علي بن هادي البشري، الجهود القانونيّة للحد من من جرائم الحاسب الآلي، مكتبة ملك فهد الوطنيّة، الطبعة الأولى، الرياض، 2005، ص 65 ـ 66..

[2] الاختراق هو القدرة على الوصول لهدف معين بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بالهدف، أو الوصول إلى البيانات الموجودة على الأجهزة الشخصية بوسائل غير مشروعة. انظر: رامي عبد العزيز، الفيروسات وبرامج التجسس ، دار البراءة ، الإسكندرية ، 2005 ، ص 82 .

[3] وهي السرقة الآلية لجزء قليل من الأرصدة باستخدام اسم وهمي أو اسم شريك، مع إمكانية التغيير مؤقتا من حساب لآخر بصفة مستمرة على شكل دائري لتقليل فرص الاكتشاف بحيث توزع الخسائر القليلة على عدد كبير من أصحاب الأرصدة بحيث لا يأبه الفرد بما يطرأ على رصيده انظر: د/ محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، المجلة العربية للدراسات الأمنية والتدريب، العدد الثلاثون ـ رجب 1421 هـ، نوفمبر 2000 م ، ص 339 .

[4] حصان طروادة : عبارة عن برمجة اختراق من حيث الطبيعة التقنية، ولها وجهان: الوجه الأول هو الزبون Client وأما الثاني هو الخادم(Surfer)، ينفصلان بإرسال الخادم إلى حاسوب الغير المقصود ويتمّ التعامل معه بعد ذلك، حيث يبرز في شكل مفيد إلا انه في الحقيقة له وجه آخر ضار ومدمر، ويقوم بنسخ ذاته إلى الملفات الأخرى وحتى الأماكن السرية والمشفرة. انظر: سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، 2007، ص11.

[5] من القضايا التي لفتت النظر إلى البعد الدولي للجرائم الالكترونية، قضية عرفت باسم مرض **نقص المناعة المكتسبة** (الايدز) التي حدثت في عام 1989، اثر قيام أحد الأشخاص بتوزيع عدد كبير من النسخ==

المواجهة، ويعد التعاون الدولي هو السبيل الوحيد من أجل التصدي لهذه الجرائم وذلك عن طريق إبرام المعاهدات والاتفاقيات الدولية التي تعمل على توفير جو من التنسيق بين الدول الأعضاء، الأمر الذي يكفل الإيقاع بمجرمي المعلوماتية وتقديمهم للقضاء العادل .

وتكمن أهمّ المشاكل المتعلقة بالتعاون الدولي حول الجريمة الالكترونية في انّه لا يوجد هناك مفهوم عام مشترك بين الدول حول صور النشاط المكون لهذه الجريمة، بالإضافة إلى أن نقص الخبرة لدى الشرطة وجهات الادعاء والقضاء في هذا المجال لتمحيص عناصر الجريمة أن وجدت وجمع الأدلة عنها للإدانة فيها يشكل عائقا كذلك أمام التعاون في مجال مكافحة هذا النوع من الإجرام .

وبالتالي من أجل التصدي للإجرام الالكتروني لابد أن تعمل الدول في اتجاهين :

الأول : داخلي حيث تقوم الدول المختلفة بسن القوانين الملائمة لمكافحة هذه الجرائم .

الثاني : دولي عن طريق عقد الاتفاقيات الدولية ، حتى لا يستفيد مجرمو المعلوماتية من عجز التشريعات الداخلية من ناحية وغياب الاتفاقيات الدولية التي تتصدى لحماية المجتمع الدولي من آثار هذه الجرائم من ناحية أخرى .

الفرع الثاني
أثر الطبيعة الخاصة بالجريمة الالكترونية على الإثبات الجنائي

إنّ الطبيعة الخاصة التي تتميز بها الجريمة الالكترونية، جعلتها تثير العديد من المشكلات، أهمها صعوبة اكتشاف هذه الجرائم، وان اكتشفت فان ذلك يكون بمحض الصدفة، والدليل على ذلك أن هذه الجرائم لم يكتشف منها إلا(1%) فقط من الجرائم المرتكبة، أما التي تم الإبلاغ عنها فلم تتعدّ (15%) من النسبة السابقة ، وحتى القضايا التي طرحت على القضاء لم تكن الأدلة كافية للإدانة فيها إلا في حدود الخمس[1].

==الخاصة بأحد البرامج الذي يهدف في ظاهره إلى إعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة، إلا أنّ هذا البرنامج في حقيقته كان يحتوي على فيروس (حصان طروادة)، والذي كان يترتب على تشغيله تعطيل جهاز الحاسوب عن العمل، ثم تظهر بعد ذلك عبارة على الشاشة يطلب الفاعل من خلالها مبلغ مالي يرسل على عنوان معين حتى يتمكن المجني عليه من الحصول على مضاد للفيروس، و في الثالث من فبراير من عام 1990 تم إلقاء القبض على المتهم **جوزيف بوب** في أوهايو بالولايات المتحدة الأمريكية، وتقدمت المملكة المتحدة بطلب تسليمه لها لمحاكمته أمام القضاء الانجليزي، لان إرسال هذا البرنامج قد تم من داخل المملكة ، وبالفعل وافق القضاء الأمريكي على تسليم المتهم، وتم توجيه أحدى عشرة ابتزاز إليه وقعت معظمها في دول مختلفة، إلا أن إجراءات محاكمة المتهم لم تستمر بسبب حالته العقلية، انظر: د/ نائلة عادل محمد فريد قورة، المرجع السابق، ص 53 .

[1] د/ سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت ،الطبعة الأولى، دار النهضة العربية، القاهرة، 1999، ص 95. وانظر: د/ عبد الله حسين علي محمود، المرجع السابق،==

كما أنّ هذه الطبيعة جعلت إثباتها يتسم بنوع من الصعوبة، حيث إنّ قصور الادلة التقليدية أضحى بيّنا، فإذا كان الاعتراف هو سيد الأدلة ، يليه شهادة الشهود، فضلا عن القرائن والآثار المادية الناجمة عن النشاط الإجرامي لهم دور في إثبات الجريمة التقليدية، فهذا الدور ضيّق بكثير إزاء إثبات الجريمة الالكترونية. ويرجع أسباب هذا القصور في إثبات الجرائم الالكترونية إلى ما يلي:

1 – تتمّ الجريمة الالكترونية في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم أركانها في بيئة الحاسوب والانترنت ويطلق عليها "البيئة الرقمية "، هذه الأخيرة تعكس على طبيعة الدليل الذي تنتجه مما تجعله غير مرئي، فهو عبارة عن نبضات الكترونية تنساب عبر النظام المعلوماتي مما يجعل أمر طمس الدليل ومحوه كليّا من قبل الفاعل أمرا في غاية السهولة وفي زمن قصير جدا [1]، ومن تمّ يتعذر إن لم يكن مستحيلا ملاحقته أو كشف شخصيته، لذلك يرى جانب من الفقه على ضرورة تدخل المشرع بإضافة حالة ارتكاب الجرائم الالكترونية كظرف استثنائي يسمح لرجال السلطة العامة بالقيام بضبط الأدلة عند وقوع الجريمة وبدون إذن مسبق من النيابة العامة، ذلك حماية للأدلة من المحو والتعديل من قبل الفاعل [2]، ففي إحدى الحالات التي شهدتها ألمانيا أدخل أحد الجناة في نظام حاسبته تعليمات أمنية لحماية البيانات المخزنة داخله من المحاولات الرامية إلى الوصول إليها من شانها محو هذه البيانات بالكامل بواسطة مجال كهربائي، في حالة اختراقه من قبل الغير [3].

2 – والى جانب ذلك فان للمجني عليه دورا سلبيا، فعادة ما يحجم عن الإبلاغ عن وقوع هذه الجرائم، مما يزيد من الصعوبة لا في مجال اكتشاف و إثبات الجرائم الالكترونية فحسب، بل وفي دراسة الظاهرة برمتها، وهو ما يعبر عنه بالرقم الأسود (Chiffre noire)، حيث يعوق رسم السياسة الجنائية السليمة لمواجهة الظاهرة الإجرامية المستجدة واختيار أفضل الوسائل لمواجهتها .

==ص 342. وانظر أيضا: د/ محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25 ــ 28 أكتوبر1993، ص 369.

[1] د / سعيد عبد اللطيف حسن، المرجع السابق، ص 95 وما بعدها .

[2] انظر: د/ أيمن عبد الحفيظ، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، العدد 25 يناير 2004، ص 373 .

[3] Ulrich Sieber, The International Handbook on Computer –related Economic, crime and the Infringement of Privacy, John and Sons ،1986، p 149 .

مشار إليه لدى د /هشام فريد رستم ، المرجع السابق، ص 23، .

فكثيرا من الجهات التي تتعرض أنظمتها المعلوماتية للانتهاك تعمد إلى عدم الكشف عنها، حتى بين موظفيها لما تعرضت له وتكتفي باتخاذ إجراءات إدارية داخلية دون الإبلاغ عنها للسلطات المختصة، تجنبا للإضرار بسمعتها ومكانتها واهتزاز ثقة عملائها فيها، لاسيما أن هذه الجرائم تقع بصفة كبيرة على المؤسسات المالية مثل البنوك والمؤسسات الادخارية والسمسرة [1]. كما يمكن أن يكون مقصد المتضرر من وراء هذا الإحجام في إخفاء أسلوب الذي ارتكبت به الجريمة لكي لا يتمّ تقليدها من الآخرين [2] .

هذا وقد أوصى المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات والذي عقد في ريو دي جانيرو بالبرازيل في الفترة من(4 ـــ 9 سبتمبر 1994)، بضرورة تشجيع المجني عليهم في هذه الجرائم على الإبلاغ عنها فور وقوعها، وذلك بهدف تخفيض الرقم الأسود للجرائم الالكترونية في الفضاء الافتراضي وهو ما قد أوصى به المجلس الأوروبي[3].

3 – بالإضافة إلى ذلك فان نقص الخبرة الفنية والتقنية لدى سلطات الاستدلال والتحقيق والقضاء يشكل عائقا أساسيًا أمام إثبات الجريمة الالكترونية ذلك أنّ هذا النوع يتطلب تدريب وتأهيل هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والملاحقة في بيئة الحاسوب والانترنت، ونتيجة لنقص الخبرة والتدريب كثيرا ما تخفق أجهزة أنفاد القانون في تقدير أهمية هذه الجرائم، فلا تبذل لكشف غموضها وضبط مرتكبيها جهودا تتناسب وهذه الأهمية ، بل أن المحقق قد يدمر الدليل عن خطأ منه أو إهمال أو بالتعامل بخشونة مع مختلف الوسائط التي تضمن الدليل كالأقراص المرنة وغيرها [4] .

---

[1] تشير بعض التقديرات أن مابين 20 و 25 % من جرائم الحاسبات لا يتم الإبلاغ عنها مطلقا خشية الإساءة للسمعة، و في دراسة أجريت على ألف شركة من الشركات المنتجة لجهاز (Fortune 500) أظهرت نتائجها أن 2% فقط من كل جرائم الحاسب هي التي تمّ الإبلاغ عنها للشرطة أو لمكتب التحقيقات الفدرالي. انظر: د/ هشام محمد فريد رستم ، نفس المرجع، هامش ص 25 .

[2] د/ زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي ، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي ، القاهرة، 25 ـــ 28 أكتوبر1993، ص 476 .

[3] من الاقتراحات التي طرحت لحمل المجني عليه على التعاون مع السلطات في الولايات المتحدة الأمريكية مطالبة البعض بأن تفرض النصوص المتعلقة بالجرائم الالكترونية التزاما على عاتق موظفي الجهة المجني عليها بالإبلاغ عما يصل علمهم به من جرائم في هذا المجال، مع تقرير جزاء على الإخلال بهذا الالتزام وعرض ذات الاقتراح على لجنة خبراء مجلس أوروبا ولاقت الفكرة رفضا باعتبار أنه ليس مقبولا تحويل المجني عليه إلى مرتكب الجريمة . انظر: د / هشام محمد فريد رستم ، المرجع السابق ، ص 25 ـــ 27 .

[4] د/ عبد الفتاح بيومي حجازي ، الدليل الجنائي و التزوير في جرائم الكمبيوتر والانترنت ـــ دراسة متعمقة في جرائم الحاسب الآلي الانترنت ـــ دار الكتب القانونية، مصر، المحلة الكبرى ،2002 ص 28 ـــ 29 .

المطلب الثاني

مفهوم الدليل الالكتروني

نظرا للطابع الخاص الذي تتميّز به الجريمة الالكترونيّة، فقد تبيّن من خلال ما سبق ذكره أنّ إثباتها يحيط به الكثير من الصعاب، ولا شكّ أنّ كشف ستر هذا النوع من الجرائم يحتاج إلى أدلة ذات طبيعة خاصة، ومختلفة عما ألفناه في الجرائم التقليديّة، حيث تستخدم فيها ذات الطبيعة التقنيّة الناجمة عن الحاسوب والانترنت، وتتمثل في **الدليل الالكتروني** (**Electronic evidence**). بمعنى آخر ترتكز عمليّة الإثبات الجنائي للجرائم الالكترونيّة على الدليل الالكتروني باعتباره الوسيلة الوحيدة لإثبات هذه الجرائم، وهو محور اهتمام بحثنا، لذا سنتناول في هذا المطلب تحديد مفهوم الدليل الالكتروني(الفرع الأول)، وما يتميّز به من خصائص(الفرع الثاني)، فضلا عن دراسة أهم تقسيمات هذا الدليل (الفرع الثالث) وذلك من خلال الفروع التاليّة:

الفرع الأول

تعريف الدليل الالكتروني

سنحاول في هذا الفرع توضيح مفهوم الدليل الجنائي بصفة عامة (أوّلا)، بهدف التعرف على الدليل الالكتروني(ثانيّا)، حيث يتعذر دراسة هذا الفرع دون المرور بالأصل.

أوّلا ـ فكرة عامة عن الدليل الجنائي :

__الدليل لغة__ : هو المرشد وما يتمّ به الإرشاد، وما يستدل به، والدليل هو الدال أيضا، والجمع أدلة و دلالات [1] ، وورد في مختار الصحاح أن الدليل ما يستدل به، وقد دلّه على الطريق أي أرشده، يدُله بالضم، دلالة بفتح الدال و كسرها و دلولة بالضم و الفتح أعلى، ويقال أدل، والاسم الدال بتشديد اللام، فلان يدل فلانا أي يثق به، قال أبو عبيد : الدال قريب المعنى من المعنى من الهدى وهما في السكينة والوقار في الهيئة و المنظر وغير ذلك [2].

---

[1] د/ جميل صليبا ، المعجم الفلسفي، دار الكتاب اللبناني، بيروت، الطبعة الأولى سنة 1970 ، ص 23 .

[2] محمد بن أبي بكر بن عبد القادر الرازي، مختار الصحاح، المطبعة الأميرية، القاهرة، 1338 هـ ، ص 209 .

والدليل اصطلاحا: هو ما يلزم من العلم به شيء آخر، وغايته أن يتوصل العقل إلى التصديق اليقيني بما كان يشك في صحته، أي التوصل به إلى معرفة الحقيقة [1].

أمّا **الدليل في الاصطلاح القانوني**، قد تعدّدت المحاولات الفقهية في وضع تعريف له [2]، حيث عرّفه البعض بأنّه: "الوسيلة التي يستعين بها القاضي للوصول إلى الحقيقة التي ينشدها". والمقصود بالحقيقة في هذا السياق هو كل ما يتعلق بالوقائع المعروضة على القاضي لإعمال حكم القانون عليها [3] . كما قيل بان الدليل :"هو الواقعة التي يستمد منها القاضي البرهان على إثبات اقتناعه بالحكم الذي ينتهي إليه [4]. فإذا نظرنا إلى هذين التعريفين نجد أن التعبير عن الدليل بأنه الوسيلة أدق من التعبير عنه بأنه الواقعة لان هذا الأخير يطلق على الجريمة نفسها لا على دليل إثباتها وأمّا الوسيلة فتطلق على ما يتوصل به إلى الشيء وهو عمل الدليل [5]

تأسيسا على ما تقدم يمكننا القول بأن الدليل الجنائي هو معلومة يقبلها المنطق والعقل يتم الحصول عليها بإجراءات قانونية لإثبات صحة افتراض ارتكاب شخص للجريمة أو دحضه ، وذلك لرفع أو خفض درجة اليقين والاقتناع لدى القاضي في واقعة محل الخلاف.

---

(1) د/ أحمد أبو القاسم ، الدليل الجنائى ودوره فى إثبات جرائم الحدود والقصاص ، بحث منشور بالمركز العربى للدراسات الأمنية والتدريب، الرياض ، 1991، ص 174

(2) د/ محمد محي الدين عوض، الإثبات بين الازدواج والوحدة، مطبوعات جامعة القاهرة بالخرطوم، 1974، هامش رقم (2)، ص 7 وما بعدها . وانظر أيضا: د / رمسيس بهنام ، المحاكمة والطعن في الأحكام، منشأة المعارف ، 1993، رقم 33 ، ص 58 و ما بعدها . انظر كذلك د / محمد زكي أبو عامر، القيود القضائية على حرية القاضي الجنائي في الاقتناع ، مجلة القانون والاقتصاد، سنة 51 ، 1981، ص 114 . وانظر أيضا: د/ برهامي أبوبكر عزمي، الشرعية الإجرائية للأدلة العلمية، دراسة تحليلية لأعمال الخبرة، دار النهضة العربية ، القاهرة ، 2006 ، ص 89 وما بعدها .

(3) د/ أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربية، القاهرة، الطبعة الثانية، 1981، ص 418.

(4) د/ مأمون سلامة، الإجراءات الجزائية في التشريع المصري، دار النهضة العربية، القاهرة، 1992، ص 191 .

(5) قد يخلط البعض أحيانا بين الدليل الجنائي و الإثبات لما بينهما من علاقة في الإجراءات القضائية ، ولكن في الواقع يمكننا الفصل بينهما كالتالي: فكلمة الإثبات بالمعنى العام يمكن أن تطلق على كل المراحل التي تمر بها العملية الاثباتية بدءا من جمع عناصر التحقيق و الدعوى تمهيدا لتقديم المتهم لسلطة التحقيق الابتدائي، فإذا أسفر هذا التحقيق عن دليل أو أدلة ترجح معها إدانة المتهم قدمته إلى المحكمة، فإذا اقتنعت بتوافر أدلة إدانة، أدانته وإلا حكمت له بالبراءة في حالة الشك طبقا لقاعدة الشك يفسر لصالح المتهم ، ومن ثم ساد القول بان الإثبات : هو تنقيب عن الدليل وتقديمه وتقديره لاستخلاص السند القانوني للفصل في الدعوى . أما الدليل هو المحصلة النهائية لكل مراحل الإثبات المختلفة ، بمعنى هو ثمرة الإثبات. لهذا يبدو واضحا أن مفهوم الإثبات أوسع من أن ينحصر في كلمة دليل . انظر: د / أحمد أبو القاسم، المفهوم العلمي والتطبيقي للدليل الجنائي المادي، مجلة مركز بحوث الشرطة، العدد السابع و العشرون ، يناير 2005 ، ص 152 .

وعلى ذلك فالدليل في المواد الجنائيّة أهميّة عظيمة لأنه هو الذي يناصر الحقيقة ويبيّن مرتكب الجريمة، وهو الذي يحوّل الشك إلى يقين، فالحقيقة في معناها العام تعني معرفة حقيقة الشيء بأن يكون أو لا يكون، وهذا لا يتحقّق إلاّ بالدليل بحسبان أنّه المعبّر عن هذه الحقيقة.

ثانيًا ـ تعريف الدليل الالكتروني :

تعدّدت التعريفات التي قيلت بشأن الدليل الالكتروني وتباينت بين التوسع والتضييق، ويرجع ذلك لموضع العلم الذي ينتمي إليه هذا الدليل، فاختلفت بين أولئك الباحثين في مجال التقنية، والباحثين في المجال القانوني، وسنحاول فيما يلي عرض أهم هذه التعريفات:

عرّف البعض الدليل الالكتروني بأنه " **كل بيانات يمكن إعدادها أو تخزينها في شكل رقمي بحيث تمكن الحاسوب من انجاز مهمة ما** " (1) . وهناك من يعرفه بأنه " **الدليل الذي يجد له أساسا في العالم الافتراضي ويقود إلى الجريمة** " (2). أو أنّه " **معلومات يقبلها المنطق والعقل ويعتمدها العلم، يتمّ الحصول عليها بإجراءات قانونية وعلمية بترجمة البيانات الحسابية المخزنة في أجهزة الحاسب الآلي و ملحقاتها وشبكات الاتصال، ويمكن استخدامها في أيّ مرحلة من مراحل التحقيق أو المحاكمة لإثبات حقيقة فعل أو شيء له علاقة بجريمة أو جان أو مجني عليه**" (3). أو ": **هو ذلك الدليل المشتق من أو بواسطة النظم البرامجية المعلوماتية الحاسوبية، وأجهزة ومعدات وأدوات الحاسب الآلي، أو شبكات الاتصال من خلال إجراءات قانونية وفنية، لتقديمها للقضاء بعد تحليلها علميّا أو تفسيرها في شكل نصوص مكتوبة أو رسومات أو صور وأشكال وأصوات لإثبات وقوع الجريمة لتقرير البراءة أو الإدانة فيها** (4) . أما الأستاذ كيسي (Casey) فيعرّف الأدلة الجنائية الرقمية بأنها " **تشمل جميع البيانات الرقمية التي يمكن أن تثبت أنّ هنالك جريمة قد ارتكبت، أو توجد علاقة بين الجريمة والجاني أو بين الجريمة والمتضرر منها. والبيانات الرقمية هي**

(1) Christin Sgarlata and David J Byer ، The Electronic paper Trail: Evidentiary Obstacles to Discovery of electronic Evidence . Journal of Science and Technology Law . 22 September 1998 .p 4.

مشار إليه عند: د/ عمر محمد أبوبكر بن يونس ، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس، 2004، ص 969.

(2) د / عمر محمد أبوبكر بن يونس، نفس المرجع، ص 969 .

(3) د/ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى ، المرجع السابق، ص 234 .

(4) عبد الناصر محمد محمود فرغلي و د/ عبيد سيف سعيد المسماري، ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، " الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية و الفنية"، دراسة تطبيقية مقارنة ، الرياض ، المنعقد في الفترة : 02 ــ 11/04 / 1148 هــ الموافق لــ 12 ــ 14 / 11 / 2007 م، ص 13.

مجموعة الأرقام التي تمثل مختلف المعلومات، بما فيها النصوص المكتوبة، الرسومات، الخرائط، الصوت و الصورة[1]. أما التعريف المقترح للدليل الالكتروني من قبل المنظمة الدولية لأدلة الحاسوب (International Organization of Computer Evidence) [2](IOCE) بأنه" **المعلومات المخزنة أو المتنقلة في شكل ثنائي، ويمكن أن يعتمد عليها في المحكمة**" [3].

وهو نفس المعنى تقريبا المتبني من قبل الفريق العلمي العامل على مستوى الأدلة الرقمية Standard Working Group on Digital Evidence (SWGDE) [4]، باعتبار هذا الأخير أنشئ من أجل توحيد الجهود التي تقوم بها المنظمة الدولية لأدلة الحاسوب (IOCE)، وتطوير مختلف التخصصات والمبادئ التوجيهية من أجل استرداد، المحافظة ودراسة الأدلة الرقمية بما فيها الصوتية والمصورة [5].

بعد استعراضنا للتعريفات التّي قيلت بشأن الدليل الالكتروني، نلاحظ في البداية أنها متقاربة من بعضها البعض، وأنّها حاولت استيعاب هذا النوع المستحدث من الدليل بالرغم من حداثته وارتباطه بالتقنية الرقمية، إلاّ أنّ هناك بعض الملاحظات ينبغي الإشارة إليها في هذا المقام تتمثل فيما يلي:

---

(1) " Digital Evidence encompasses any and all digital data that ran establish that a crime has been committed or can provide a link between a crime and its victim or acrime and its perpetrator . This Digital Data is a combination of numbers that represent information of various kinds ، including text ، images ، audio ،and video . By Eoghan Casey ،Digital Evidence and Computer Crime—Forensic Science، Computers and the Internet ، Second Edition ، Academic Press An imprint of Elsevier ، London ، 2004 ، p 260 .

(2) المنظمة الدولية لأدلة الحاسوب (IOCE) هي: تنظيم دولي تمّ اعتماده في نسيان/ أبريل 1995، مقره الولايات المتحدة الأمريكية، وتسعى هذه المنظمة إلى توفير منتدى دولي لوكالات أنفاد القانون لتبادل المعلومات بشأن التحقيق في جرائم الحاسوب وغيرها من قضايا الطب الشرعي، ويتألف من أجهزة إنفاذ القانون والوكالات الحكومية المعنية بالتحقيق الرقمي وتحقيقات الطب الشرعي، وذلك بناء دعوة من المجلس التنفيذي بالمنظمة . لمزيد من التفصيل حول المنظمة يرجى العودة للموقع الخاص بها وهو كالتالي :
Http: //www.ioce.org/ index? php id =15

(3) - Electronic evidence is" information stored or transmitted in binary form that may be relied upon in court ". Eoghan Casey, op. cit , p. 261.

(4) عرّف الفريق العلمي العامل على مستوى الأدلة الرقمية الدليل الرقمي بأنه" **المعلومات المخزنة أو المتنقلة في شكل ثنائي ، ذات قيمة اثباتية**".

" Digital Evidence is any information of probative value ، that is either stored or transmitted in a digital form" .

(5) لمزيد من التفصيل حول الفريق العامل حول مستوى الأدلة الرقمية، انظر الموقع التالي :
www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

1 – هناك خلط في تعريف الدليل الالكتروني بمفهوم برامج الحاسب الآلي عند بعض الفقهاء[1]، حيث تمّ اعتبار هذا الدليل كبيانات يتمّ إدخالها إلى جهاز الحاسوب، وذلك لانجاز مهمة ما، وهذا التعريف ينطبق تماما مع مفهوم برامج الحاسب الآلي[2].

صحيح قد يتفق المصطلحان في أنّ كليهما يعدّا آثارا معلوماتية أو رقمية، حيث يتركهما كل مستخدم للنظام المعلوماتي، ويتّخذ شكلا واحدا هو الشكل الرقمي، لأنّ البيانات داخل الكمبيوتر سواء كانت في شكل نصوص أم أحرف، أرقام، رموز، أصوات أو صور تتحوّل إلى طبيعة رقمية، لان تكنولوجيا المعلومات الحديثة ترتكز على تقنية الترقيم، التي تعني ترجمة أو تحويل أي مستند معلوماتي مؤلف من نصوص أو صور ..إلى نظام ثنائي في تمثيل الأعداد يفهمه الكمبيوتر قوامه الرقمان [صفر]، واحد] [3]. بل أكثر من ذلك قد تعدّ بعض البرامج لوحدها دليلا إلكترونيا مثل برنامج الاختراق (**asylu_014_fe**)[4]

إلاّ أنّ الفرق بين الدليل الالكتروني وبرامج الحاسوب يكمن في الوظيفة التي يؤديها كل واحد منهما، فهذا الأخير له دور في تشغيل الحاسوب وتوجيهه إلى حلّ المشاكل ووضع الخطط المناسبة، وبدونها لا يعدو أن يكون مجرد آلة صماء كباقي الآلات، بل انه توجد

---

[1] عند Christin Sgarlata and David J Byer. انظر فيما سبق ص 30 .

[2] تعد برامج الحاسوب من أهم المكونات المنطقية للحاسوب وهي بمثابة العمود الفقري له، ولها مفهومان أحدهما ضيق والآخر واسع. فالمدلول الضيق ينصرف إلى" مجموعة التعليمات الموجهة من الإنسان إلى الآلة والتي تسمح لها بتنفيذ مهمة معينة". أمّا المدلول الواسع فيشمل فضلا عن المفهوم الضيق للبرامج، التعليمات والأوامر الموجهة للعميل مثل بيانات استعمال البرنامج وكيفية المعالجة الالكترونية للمعلومات، أي كافة البيانات الأخرى الملحقة بالبرنامج والتي تساعد على سهولة فهم تطبيقه، وهذه البيانات عبارة عن تعليمات موجهة من المبرمج الذي يتولى إعداد البرنامج إلى العميل الذي يتعامل مع الآلة. انظر: محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر،2002، ص 33 وما بعدها. وانظر أيضا: د/ علي عبد القادر القهوجي, الحماية الجنائيّة لبرامج الحاسب الآلي, دار الجامعة الجديدة للنشر, 1997, ص 5. وانظر كذلك: محمد مسعود خليفة, الحماية الجنائيّة لمعطيات الحاسب الآلي في القانون الجزائري والمقارن, رسالة ماجيستير, كليّة الحقوق, جامعة الاسكندريّة, 2005– 2006, ص 63 وما بعدها.

[3] النظام الثنائي الرقمي (Binary)، أعتمد أساسا للكمبيوتر الرقمي ويمكن من هذا النظام تحول كافة الأرقام العشرية والحروف والأشكال إلى نظام ثنائي، ويمكن من جهة أخرى الاعتماد على المكافئ له سواء كان نظام ثنائي أو نظام الست عشر. مشار إليه عند: د/ ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، مصر، المحلة الكبرى ، 2006 ، ص 22 .

[4] والمشكلة في الوقت الحالي أنّه يمكن لأي شخص تحميل هذه الأنواع من البرامج الخطرة وبالمجان من الانترنت، مثلا يحمّل برنامج (asylu_014_fe) من الموقع التالي:
http://upload.9q9q.net/file/ghc7b6yZ...14_fe.zip.html

برامج خاصة تساهم في استخلاص الدليل الالكتروني مثل: برنامج معالجة الملفات مثل: (X tree Pro Gold)[1]، وبرنامج النسخ مثل (Lap Link)[2] .

أمّا الدليل الجنائي الرقمي له أهمية كبرى ودور أساسي في معرفة كيفية حدوث الجريمة الالكترونية، بهدف إثباتها ونسبتها إلى مرتكبيها، لاسيما في البيئة الافتراضية، غير محسوسة (intangible)، حيث يمكن تفتيش محتوى القرص الصلب لمعرفة كل المراحل التي مرّ بها المجرم وهو في سبيل تحقيقه للهدف الإجرامي.

وتجدر الإشارة إلى أنّ الدليل الجنائي الالكتروني لا يقتصر دوره في إثبات الجرائم الالكترونية فحسب، كسرقة الملكية الفكرية، واستغلال الأطفال في المواد الإباحية، والتحرّش الجنسي بل يتعداه إلى الجرائم التقليدية كالاتجار بالمخدرات وجرائم القتل والاختطاف [3] التي تستخدم فيها التكنولوجيا الرقمية كأداة لتسهيل تنفيذ الجرائم بسرعة وكفاءة قد تفوق قدرات المحققين من جهة [4]، كما يلجأ إلى هذه التقنية بغرض التستّر عن أعين الأمن [1] من جهة

---

[1] برنامج معالجة الملفات مثل(X tree Pro Gold): برنامج يُمكّن المحقق من العثور على الملفات في أيّ مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يُمكّن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

[2] برنامج النسخ مثل(Lap Link) وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر سواء على التوازي (Parallel Port) أو على التوالي (Serial Port) وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أيّ محاولة لتدميرها من جانب المتهم . انظر: د/ ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP / IP) في بحث وتحقيق الجرائم على الكمبيوتر، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية ، المنعقد في 26 ـــ 28 نيسان 2003، بدبي ـــ الإمارات العربية المتحدةـــ ، ص 10. متاح على الموقع التالي :

http://www.arablawinfo.com/research_search.asp?validate=articles&ArticleID=133

[3] للتدليل على ذلك، نشير إلى قضية اختطاف طالبة واستخدامها جنسيا، ووقعت هذه القضية في نيويورك بالولايات المتحدة الأمريكية في ابريل 1996، حيث قام شخص اسمه (أليفر جوفانوفيك) بالتحضير لمقابلة المجني عليها عبر رسائل الكترونية ، ثم وجه لها دعوة لمشاهدة أفلام مسجلة على الفيديو، وعند وصول الفتاة قام لمتهم باحتجازها لمدة (20 ساعة) واعتدى عليها بطريقة وحشية مع الضرب و الحرق و التعذيب، وفي هذا الإطار تم التعرف على شخصية المتهم عن طريق الأدلة الرقمية المضمنة في رسائل البريد الالكتروني المتبادلة بين الجاني والضحية. إلاّ انه لم يتمكن الاتهام من استخدام الأدلة الرقمية المخزنة في البريد الالكتروني للمتهم لعدم ضبطها بالطرق المشروعة، كما منع الدفاع من استخدام الأدلة الرقمية المخزنة في البريد الالكتروني للمجني عليها، لان قوانين نيويورك تمنع كشف بعض المعلومات الخاصة بالأفراد بما في ذلك التحقي من الشخصية أو كشف تاريخها الجنسي . مشار إليها عند: الدكتور/ محمد الأمين البشري، المرجع السابق، ص 257 وما بعدها. للمزيد من الأمثلة المشابهة انظر :

Eoghan Casey, op. cit, P.10.

[4] وفي ذلك يقول (كارتر وكاتز): " لقد صمدت أجهزة الشرطة خلال السنوات الماضية أمام العديد من التحديات ، الجريمة المنظمة، الشغب، تجارة المخدرات، وجرائم العنف. إلا أنها واجهت مشاكل غير==

أخرى، حيث يعتقد المجرمون أن هذه البيئة منفصلة تماما عن العالم المادي، ممّا يجعلهم يشعرون بالأمان. إلاّ أنّ هذا الاعتقاد في غير محله ذلك لانّ هناك العديد من الجرائم المرتكبة في العالم المادي لا تكون واضحة من دون الانترنت، فقد تمّ اكتشاف العديد من صفقات المخدرات تجرى على الشبكة وذلك عن طريق المراقبة الالكترونية. فيمكننا إذن معرفة المزيد عن الأنشطة الإجرامية التي توجد من حولنا في العالم المادي ــ خاصة وأن شبكة الانترنت في كثير من الأحيان ذات صلة ــ و تتضمّن الأدلة الرقمية ممّا ينبغي أن ينظر إليها على أنها امتداد لمسرح الجريمة المادي .

2 ــ حصرت التعريفات السابقة مصادر الأدلة الالكترونية في أجهزة الحاسب الآلي وملحقاتها أو ما تعرف عند التقنيين **بفُتح النظم الحاسوبية** [2]، ونظم الاتصال، إلاّ أن العلم أثبت أن هناك نظم أخرى مدمجة بالحواسيب قد تحتوي على العديد من الأدلة الرقمية كالهواتف المحمولة (Mobile Telephone) والبطاقات الذكية (Smart Cards)[3]

==عادية ومعقدة ألا وهي مشكلة الجريمة المعلوماتية، وهناك عدة عوامل تجعل من الصعب على الشرطة مواجهة هذا النوع من الإجرام. حيث قام المجرمون بالدمج بين وسائل التقنية العالية مع الجريمة التقليدية ليخرجوا لنا بأنماط جديدة ومعقدة من الجرائم، ومما يعيق المعالجة أن الأدلة المطلوبة في مثل هذه الجريمة ليست أدلة مادية ملموسة أو مشاهدة، بل هي نبضات الكترونية وبرامج مشفرة ومن المؤسف أن أجهزة الشرطة تخلفت كثيرا في مجال تقنية المعلومات، وعليها أن تستيقظ من أجل العمل الجاد لمواكبة المتغيرات. انظر :

Karer David Land Kartz .A .J . Computer Crime :An Emerging Challenge for Law Enforcement F.B.I. Bulletin 1996. (available at : http://www. fbi.gov/leb.96text)

مشار إليه عند د/ محمد الأمين البشري، المرجع السابق، 243 ــ 242.

[1] Jean-François, Plaideur en faveur d'aménagement de la preuve de l'infraction informatique, revue de science criminel et de droit pénal compare, N' 1, janvier/ mars 2004. p. 72 .

[2] **فُتح النظم الحاسوبية** تتألف من محركات الأقراص الصلبة ولوحة المفاتيح ورصد مثل الحواسيب المحمولة وشاشات الحاسوب وغيرها من النظم التي تحتوي على المعلومات المخزنة. أما نظم الاتصال فتشمل جميع أنواع الشبكات بما فيها شبكة المعلومات الدولية ــ الانترنت ــ فهي ثرية جدا من معلومات مثل صفحات المواقع المختلفة (Web Page) والبريد الالكتروني(Email)، غرف الدردشة والمحادثة (Logs of Synchronous Chat Sessions). انظر : Eoghan Casey, oP. cit , p. 2-13.

[3] البطاقة الذكية :بطاقة بلاستيكية تحتوي على شريحة إلكترونية يمكن أن يتم تخزين أي نوع من البيانات عليها سواء كانت بيانات مكتوبة أو صورا، وكذلك يمكن تحميل عدة برامج على البطاقة، ويمكن حماية المعلومات على الشريحة بعدة مستويات من السرية ابتداء من القراءة المباشرة إلى استخدام كلمة سر خاصة بحاملها أو استخدام برامج خاصة تتحكم فيها جهة الإصدار، كما تتميز البطاقة بإمكانية تغيير البيانات المخزنة على الشريحة ودون الحاجة إلى إصدار بطاقة جديدة، ولها عدة تطبيقات وذلك لتنوع البيانات التي يمكن تخزينها، مثل رخص السياقة ، مفاتيح غرف الفنادق والجوازات ..الخ . لمزيد من التفصيل انظر:==

والمساعد الرقمي الشخصي (personal digital assistants)[1].

وتأسيسا على هذه الملاحظات، واسترشادا بما سبق عرضه من تعريفات للدليل الالكتروني، يمكننا تعريفه بأنّه: "**معلومات مخزنة في أجهزة الحاسوب وملحقاتها ـ من دسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات كالطابعات والفاكس ـ أو متنقلة عبر شبكات الاتصال، والتي يتمّ تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبيها** ".

الفرع الثاني
خصائص الدليل الالكتروني

إنّ البيئة الرقمية التي يعيش فيها الدليل الالكتروني بيئة متطورة بطبيعتها، فهي تشمل على أنواع متعددة من البيانات الرقمية تصلح منفردة أو مجتمعة لكي تكوّن دليلا للإدانة أو البراءة، وقد انعكس هذا العالم الرقمي على طبيعة هذا الدليل ممّا جعله يتّصف بعدة خصائص ميّزته عن الدليل الجنائي التقليدي وهي كالتالي :

1ـ الدليل الالكتروني دليل علمي: يتكوّن هذا الدليل من بيانات ومعلومات ذات هيئة الكترونية غير ملموسة لا تدرك بالحواس العادية، بل يتطلب إدراكها الاستعانة بأجهزة ومعدات، وأدوات الحاسبات الآلية، واستخدام نظم برامجية حاسوبية، فهو يحتاج إلى مجال تقني يتعامل معه، وهذا يعني أنه كدليل يحتاج إلى بيئته التقنية التي يتكوّن فيها لكونه من طبيعة تقنية المعلومات، ولأجل ذلك فان ما ينطبق على الدليل العلمي ينطبق على الدليل الالكتروني. فالدليل العلمي

== د/ محمد محمد محمد عنب، موسوعة العلوم الجنائية، تقنية الحصول على الآثار والأدلة المادية، الجزء الأول، مركز بحوث الشرطة، الشارقة، الطبعة الأولى، 2007، ص 701 و ما بعدها .
وانظر الموقع التالي:
http://www.alsharq.com/PrintPage.aspx?xf=2008،February،article_20080220_685&id=ocal&sid=localnewsl

[1]ـ المساعدات الرقمية الشخصية (Personal Digital Assistants) ويطلق عليها أيضا (PDAs) هي أجهزة حاسوب محمولة باليد (Handheld Devices) أو توضع في الجيب، صممت في البداية لاستخدامها في تنظيم المواعيد الشخصية، وتخزين هواتف الأصدقاء وعناوينهم، وتسجيل البيانات الخاصة، وكتابة الملاحظات أثناء المحاضرات أو الاجتماعات، وقوائم بالمهام (Task Lists).
وتقسم معظم المساعدات الرقمية الشخصية إلى نوعين رئيسيين هما: أجهزة الحاسوب الكفيّة (Handheld PC) أو (Palm top) ، وأجهزة حاسوب الجيب (Pocket PC) . لمزيد من التفصيل انظر: د/ محمد محمد محمد عنب ، المرجع السابق، ص 714 ، وانظر أيضا الموقع التالي :
http://www.zu.edu.eg/users/ahmedsalem/page.asp?id=58

يخضع لقاعدة لزوم تجاوبه مع الحقيقة كاملة وفقا لقاعدة في القانون المقارن(**إن القانون مسعاه العدالة أما العلم فمسعاه الحقيقة**)، وإذا كان الدليل العلمي له منطقه الذي لا يجب أن يخرج عليه، إذ يستبعد تعارضه مع القواعد العلمية السليمة، فانّ الدليل الالكتروني له ذات الطبيعة، فلا يجب أن يخرج هذا النوع من الأدلة عما توصل إليه العلم الرقمي وإلا فقد معناه[1].

2- **الدليل الالكتروني دليل تقني**: فهو مستوح من البيئة التي يعيش فيها وهي البيئة الرقمية أو التقنية، وتتمثل هذه الأخيرة في إطار الجرائم الالكترونية في العالم الافتراضي، وهذا العالم كامن في أجهزة الحاسب الآلي والخوادم والمضيفات والشبكات بمختلف أنواعها. فالأدلة الرقمية ليست مثل الدليل العادي، فلا تنتج التقنية سكينا يتمّ به اكتشاف القاتل أو اعترافا مكتوبا أو بصمة أصبع ..، وإنّما تنتج التقنية نبضات رقمية تصل إلى درجة التخيلية في شكلها وحجمها ومكان تواجدها غير المعلن، فهي ذات طبيعة ديناميكية فائقة السرعة تنتقل من مكان لآخر عبر شبكات الاتصال متعدية لحدود الزمان و المكان .

3- **الدليل الالكتروني يصعب التخلص منه**: وتعدّ من أهمّ خصائص الدليل الالكتروني، بل انه يمكن اعتبار هذه الخاصية **ميزة** يتمتّع بها الدليل الرقمي عن غيره من الأدلة التقليدية [2]، حيث يمكن التخلص بكل سهولة من الأوراق والأشرطة المسجلة إذا حملت في ذاتها إقرار بارتكاب شخص لجرائم وذلك بتمزيقها وحرقها، كما يمكن أيضا التخلص من بصمات الأصابع بمسحها من موضعها، بالإضافة إلى انه في بعض الدول الغربية يمكن التخلص من الشهود بقتلهم أو تهديدهم بعدم الإدلاء بالشهادة، هذا الأمر بالنسبة للأدلة التقليدية ،أما بالنسبة للأدلة الرقمية فان الحال غير ذلك، حيث يمكن استرجاعها بعد محوها، وإصلاحها بعد إتلافها، وإظهارها بعد إخفائها، ممّا يؤدي إلى صعوبة الخلاص منها، لان هناك العديد من البرامج الحاسوبية وظيفتها استعادة البيانات التي تمّ حذفها أو إلغائها مثل **Recover Lost Data** ،**O&O Rescue Box v4.0** [3]، سواء تمّ هذا الإلغاء بالأمر(Delete) أو عن طريق إعادة تهيئة أو تشكيل للقرص الصلب (Hard Disk) باستخدام الأمر (Format)، سواء كانت هذه البيانات صورا أو رسومات أو كتابات أو غيرها، كل ذلك يشكل صعوبة أخفاء الجاني

---

[1] د/ عمر محمد ابوبكر بن يونس ، المرجع السابق، ص 977. وانظر ايضا:

Eoghan Casey ، op –cit ، p 9 .

[2] يتشابه الدليل لالكتروني مع الدليل الجيني أو ما يطلق عليه DNA، وذلك لاتحادهما في خصوصية صعوبة التخلص منهما من ناحية ، ومن ناحية أخرى يمكن إحداث تعديل في تكوينهما.

[3] لمزيد من التفصيل حول هذه البرامج انظر الموقع التالي :

http://edu.arabsgate.com/showthread.php?t=502020

لجريمته أو التخفي منها عن أعين الأمن والعدالة، طالما علم رجال البحث والتحقيق الجنائي بوقوع الجريمة . بل إنّ نشاط الجاني لمحو الدليل يشكل كدليل أيضا، فنسخة من هذا الفعل (فعل الجاني لمحو الدليل) يتمّ تسجيلها في الكمبيوتر ويمكن استخلاصها لاحقا كدليل إدانة ضده [1].

4 ـ **الدليل الالكتروني قابل للنسخ**: حيث يمكن استخراج نسخ من الأدلة الجنائية الرقمية مطابقة للأصل ولها نفس القيمة العلمية، وهذه الخاصية لا تتوافر في أنواع الأدلة الأخرى(التقليدية)، ممّا يشكل ضمانة شديدة الفعالية للحفاظ على الدليل ضد الفقد والتلف والتغيير عن طريق نسخ طبق الأصل من الدليل[2]. ومثل هذا الأمر لاحظه المشرع البلجيكي فقام بتعديل قانون التحقيق الجنائي (Code d'instruction Criminelle) بمقتضى القانون المؤرخ في (28نوفمبر2000)، حيث تمّ إضافة المادة (39 bis) **التّي سمحت بضبط الأدلة الرقمية، مثل نسخ المواد المخزنة في نظم المعالجة الآلية للبيانات بقصد عرضها على الجهات القضائية**[3].

5ـ يمتاز الدليل الالكتروني بالسعة التخزينية العالية فآلة الفيديو الرقمية، يمكنها تخزين مئات الصور، ودسك صغير يمكنه تخزين مكتبة صغيرة ..الخ [4].

6ـ الدليل الالكتروني يرصد معلومات عن الجاني ويحللها في ذات الوقت، حيث يمكنه أن يسجل تحركات الفرد، كما انّه يسجل عاداته وسلوكياته وبعض الأمور الشخصية عنه، لذا فانّ البحث الجنائي قد يجد غايته بسهولة أيسر من الدليل المادي .

هذه الخصائص سبغت على الدليل طابع متميّز، جعلته يتميّز بذاتية خاصة مختلفة عن الأدلة التقليديّة ممّا جعلتنا نتساءل عن موقع هذا الدليل من تقسيمات الدليل الجنائي بصفة عامة، وقبل الإجابة على هذه الإشكالية يتعيّن علينا عرض مختلف تقسيمات الدليل الجنائي بما يتناسب وموضوع الدراسة، لان هناك العديد المحاولات الفقهية التي حاولت وضع تصنيفات للدليل الجنائي، نذكر منها على سبيل الإيجاز ما يلي :

ـ تقسيم الدليل من حيث وظيفته إلى: أدلة اتهام، أدلة حكم، وأدلة نفي.

---

[1] د/ ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة والقانون، المجلد الخامس، المنعقد في: 10 ـ 12 مايو 2003، ص 2240.

[2] عبد الناصر محمد محمود فرغلي و د/ عبيد سيف سعيد المسماري ، المرجع السابق ، ص 15 .

[3] د/ عمر ممد ابوبكر بن يونس ، المرجع السابق، ص 978.

[4] د/ ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم، وعبد الله عبد العزيز، المرجع السابق، ص 2241 .

ـ تقسيم الدليل من حيث قيمته الاثباتية على النحو التالي:

1. الأدلة الكاملة مثل شهادة الشهود، الدليل الكتابي، القرينة، الاعتراف.
2. الأدلة الناقصة كما في حالة تواجد شهادة شاهد واحد.
3. الأدلة الضعيفة أو الخفيفة [1].
4. الأدلة غير الكافية .

- تقسيم الدليل من حيث صلته بالواقعة المراد إثباتها: إلى أدلة مباشرة كالمعاينة وشهادة الشهود والاستجواب والتفتيش. أمّا الأدلة غير المباشرة فمثالها القرائن و الدلائل .

- تقسيم الدليل من حيث الجهة التي يقدم إليها: إلى أدلة قضائية وغير قضائية، فالدليل القضائي هو الدليل الذي له مصدر في أوراق الدعوى أمام المحكمة سواء كانت في محاضر الاستدلال أم التحقيق، أمّا الدليل غير القضائي فهو ما لا يكون له أصل في الأوراق المعروضة على القاضي، كأن تكون معلومات شخصية يحصل عليها القاضي بنفسه خارج مجلس القضاء [2].

وما يهمنا في هذا المقام هو تقسيم الدليل من حيث نسبته إلى مصدره، فهو الأساس الذي نقيم عليه المقارنة بين الدليل الالكتروني و الدليل الجنائي، حيث ينقسم هذا الأخير إلى أربعة أنواع : أدلة قانونية ، وفنية وقوليه ، ومادية ، وسنعرض فيما يلي أهم السمات المميزة لهذه التقسيمات:

1ـ **الدليل القانوني:** ويقصد به الأدلة التي حدّدها المشرع وعيّن قوة كل منها، بحيث لا يمكن الإثبات بغيرها، وهو الأصل في المواد المدنية، أمّا في المسائل الجنائية فانّ الأدلة غير محصورة، والقاضي حرّ في تكوين عقيدته من أيّ دليل في الدعوى، لكن في بعض الحالات يورد القانون استثناءات معينة على حريّة القاضي في الإثبات والاقتناع فيمنع عليه الأخذ بدليل معين، أو يمنع من الحكم بالإدانة إلاّ إذا توافرت لديه أدلة معينة [3]، كما في حالة إثبات

---

[1] وهذه الأدلة تجعل المتهم من خلالها في وضع الاشتباه أي لا يحكم عليه بالإدانة ولا بالبراءة، وإنما يحكم بتوسطهما ويطلق عليه " Mishers de cour "، فهذا الاشتباه يفتح باب التحقيق ولكن من الممكن أن تكون أدلة مكملة لغيرها تخول القاضي الاستناد إليها في الحكم بالإدانة. انظر: د/ محمود محمود مصطفى،الإثبات في المواد الجنائية في القانون المقارن، الجزء الأول، النظرة العامة، مطبعة جامعة القاهرة والكتاب الجامعي، الطبعة الأولى، 1977، ص 9 .

[2] د/ أحمد أبو القاسم، المفهوم العلمي والتطبيقي للدليل الجنائي المادي، المرجع السابق، 2005، ص 162.

[3] د/ هلالي عبد الله أحمد، النظرية العامة للإثبات في المواد الجنائية ــ دراسة مقارنة بالشريعة الإسلامية ــ رسالة دكتوراه، كلية الحقوق، جامعة القاهرة ، سنة 1984 ، ص 349 .

المسائل غير الجنائية (المسائل الأولية) وفي حالة إثبات عقود الأمانة في خيانة الأمانة، وإثبات الزنا على شريك الزوجة الزانية [1].

2ـ **الدليل الفني:** ويقصد بهذا النوع من الأدلة ذلك الدليل الذي ينبعث من رأي الخبير الفنّي حول تقدير دليل مادي أو قولي قائم في الدعوى، وفق معايير ووسائل علميّة معتمدة، و يتمثل عادة في الخبرة التي هي عبارة عن تقارير فنيّة تصدر عن الخبير بشأن رأيه الفنّي في وقائع معينة [2].

3 ـ **الدليل القولي:** هو الدليل الذي ينبعث من أشخاص أدركوا معلومات مفيدة للإثبات بإحدى حواسهم، وتتمثّل في الاعتراف وأقوال الشهود، وقد يسمّيها البعض بالأدلة المعنوية أو النفسية .(Verbal Evidence)

4 ـ **الدليل المادي:** هو الدليل الناتج من عناصر مادية ناطقة بنفسها وتؤثّر في اقتناع القاضي بطريقة مباشرة [3]، أو هو "حالة قانونية منطقية تنشأ من استنباط أمر مجهول من نتيجة فحص علمي أو فنّي لأثر مادي تخلّف عن جريمة وله من الخواص ما يسمح بتحقيق هويّته أو ذاتيته والربط بينه وبين معطيات التحقيق في تساند تام" [4]. وقد حظي هذا النوع من الأدلة بالدراسة من قبل العديد من الفقهاء والباحثين[5]، خاصّة أنه يرتبط بشكل مباشر بالوسائل العلمية الحديثة في مجال كشف الجريمة .

فأين تقع الأدلة الالكترونية من بين هذه الأنواع ؟ هل تعتبر الأدلة الرقمية أدلة مادية لكونها ناتجة من عناصر مادية ملموسة و تستخدم العلم ونظرياته لاستخلاصها ؟ أم تعتبر من الأدلة الفنية لانبعاثها من رأي خبير فني ووفق معايير علمية معتمدة ؟ .

يمكن إجمال المواقف الفقهية فيما يخص تحديد طبيعة الأدلة الالكترونية وموقعها من الأدلة الجنائية بصفة عامة إلى اتجاهين اثنين نعرضهما في ما يلي :

---

[1] لمزيد من التفصيل انظر: د/ محمود محمود مصطفى، المرجع السابق، ص 90و ما بعدها.

[2] د/ احمد فتحي سرور، المرجع السابق، ص 346. وانظر أيضا: د/ عبد الحكم فوده، حجية الدليل الفني في المواد الجنائية و المدنية ــ دراسة علمية على ضوء قضاء النقض ــ دار الألفي لتوزيع الكتب القانونية بالمنيا ، بدون تاريخ الطبع، ص 7 و ما بعدها .

[3] د / محمد الأمين البشري، المرجع السابق ، ص 234.

[4] د/ أحمد أبو القاسم ، المرجع السابق، ص 17 .

[5] د/ أحمد أبو القاسم، الدليل المادي ودوره في الإثبات في الفقه الجنائي الإسلامي ــ دراسة مقارنة ــ دار النهضة العربية، 1991، ص 180 و ما بعدها. وانظر أيضا: د/ زين العابدين سليم ، الدليل المادي سيد الأدلة، مجلة الأمن العام، العدد65، أبريل سنة 1974، ص 73. د/ معجب معدي الحويقل، دور الأثر المادي في الإثبات الجنائي، أكاديمية نايف العربية للعلوم الأمنية ،الطبعة الأولى ، الرياض، ص 9 وما بعدها.

- **الاتجاه الأول:** يرى أنصار هذا الاتجاه أنّ الأدلة الجنائية الرقميّة ما هي إلاّ مرحلة متقدّمة من الأدلة المادية الملموسة التي يمكن إدراكها بإحدى الحواس الطبيعية للإنسان إذا ما كانت على شكل مطبوعات مستخرجة من الحاسوب، باعتباره مصدر الدليل الالكتروني، فالأدلة الجنائية الرقمية في منظور هذا الاتجاه لا تختلف من حيث المفهوم والقيمة عن آثار الأسلحة وبصمات الأصابع والبصمة الوراثية (DNA) وغيرها من الأدلة العلمية [1].

إلاّ أنّ بعض الفقهاء [2] قد حدّد حالات من الأدلة لا تعتبر دليلا ماديا وهي الأدلة المستمدة سواء من:

1 - الوسائل التي تمسّ سلامة جسم الإنسان، وصحته النفسية وتكشف أسراره الوجدانية، مثل وضع الإنسان تحت جهاز كشف الكذب، واستخدام وسائل التحليل التخديري وأمصال الحقيقة، وكذلك استخدام التنويم المغناطيسي واستخدام جهاز رسم المخ الكهربائي.

2 - أو من الوسائل السمعية والبصرية التي قد يترتّب على استخدامها تعدّ على الحياة الخاصة للإنسان كمراقبة وتسجيل المحادثات التليفونية، وأجهزة التصنت، وأجهزة التسجيل الصوتي والتلفزيوني والتصوير باستخدام العدسات المقربة وغيرها، فاستبعاد هذه الأدلة يقوم على أساس أنها لا تعتبر أثرا ماديا ملموسا تصلح للمعالجة الفيزيائية لتحديد أبعادها، وان استندت إلى أساليب ووسائل علمية، بِغضّ النظر عن موقف الفقه القانوني من مشروعيتها، وهذا الأساس ينطبق تماما على الدليل الالكتروني باعتباره مجرد نبضات كهرومغناطيسية غير ملموسة، لا تدرك بالحواس العادية، بل يتطلّب إدراكها الاستعانة ببرامج و تطبيقات خاصة .

وعلى عكس هذا الاتجاه، يذهب أنصار **الاتجاه الثاني**[3]، إلى القول بأنّ الأدلة الرقمية نوع متميّز من وسائل الإثبات ولها من المواصفات ما يؤهلها لتقوم كإضافة جديدة لأنواع الأدلة الجنائية الأربعة (القانونية، الفنية، القولية، والمادية) ونحن بدورنا نؤيده في ذلك، لان الأدلة الالكترونية تتمتّع بخصائص جعلتها متميزة عن غيرها من الأدلة الجنائية الأخرى سواء من حيث البيئة التي تنبعث منها وهي العالم الافتراضي المبني على الكيفية المعنوية غير الملموسة (Intangible)، وهذا الأمر يشكل قالب الدليل الالكتروني في تكنولوجيا المعلومات،

---

(1) Eoghan Casey, op.cit , p.5.

(2) الدكتور/ أحمد أبو القاسم ، المرجع السابق ، ص 17 .

(3) من بينهم **اللواء الدكتور محمد الأمين البشري**، في مؤلفه التحقيق في الجرائم المستحدثة ، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية ، الرياض ، سنة 2004، ص 235.

أو من حيث الشخص القائم على جمعه حيث يشترط فيه على الأقل أن يكون ملمّا بتقنية المعلومات.

فهذه الطبيعة الخاصة بالدليل الالكتروني دفعت الولايات المتحدة الأمريكية إلى إنشاء المنظمة الدولية لأدلة الحاسوب (IOCE) International Organization of (Computer Evidence، ورافقته بذلك الفريق العامل على مستوى الأدلة الرقمية Standard Working Group on Digital Evidence (SWGDE) حيث أنشئ هذا الفريق من أجل توحيد الجهود التي تقوم بها هذه المنظمة، كما تمّ وضع المجلة الدولية للأدلة الرقمية (International Journal of Digital Evidence) (IJDE)[1]، وذلك دليل على تميّز الأدلة الالكترونية عن الأدلة الجنائية التقليدية و بالتالي أهمية هذه الأدلة في مجال التحقيق الجنائي بصفة عامة والتحقيق الجنائي الرقمي على وجه الخصوص.

الفرع الثالث
تقسيمات الدليل الالكتروني

تختلف الجريمة الالكترونية عن الجريمة التقليدية في كون الأولى تتمّ في بيئة غير مادية عبر نظام حاسب آلي أو شبكة المعلومات الدولية ـ الانترنت ـ حيث يمكن للجاني عن طريق نبضات الكترونية رقميّة لا ترى أن يعبث في بيانات الحاسوب أو برامجه وذلك في وقت قياسي قد يكون جزءا من الثانية، كما يمكن محوها في زمن قياسي قبل أن تصل يد العدالة إليه إذا ما استخدمت برامج خاصة في ذلك، ممّا يصعب الحصول على دليل مادي في مثل هذه الجرائم، حيث تغلب الطبيعة الالكترونية على الدليل المتوافر. إلاّ أنّ لهذا الأخير ميزة التنوع فلا يأتي على صورة واحدة بل يوجد له العديد من الصور والأشكال، وفي هذا الصدد نلمس نوعين من التقسيمات للأدلة الالكترونية نبينها في الآتي :

أولا ـ المحاولات الفقهية لتقسيم الدليل الالكتروني:

لم يتطرّق فقهاء القانون الجنائي إلى دراسة الأدلة الكترونية بشكل واسع، ويرجع ذلك إلى الحداثة النسبية لهذه الأدلة من جهة، والتطور المتلاحق الذي يطرأ على العالم الرقمي من

---

[1] لمزيد من التفصيل حول المجلة الدولية للأدلة الرقمية انظر الموقع الخاص بها :
http://www.utica.edu/academic/institutes/ecii/publications/ijde.cfm

ناحية أخرى، وسوف نتطرق إلى محاولة فقهية[1]، تمّ تقسيم الدليل الالكتروني بموجبها إلى أربعة أقسام تتمثّل فيما يلي:

القسم الأول : الأدلة الرقمية الخاصة بأجهزة الكمبيوتر و شبكاتها .

القسم الثاني : الأدلة الرقمية الخاصة بالانترنت .

القسم الثالث : الأدلة الرقمية الخاصة ببرتوكولات تبادل المعلومات بين أجهزة الشبكة العالمية للمعلومات.

القسم الرابع : الأدلة الرقمية الخاصة بالشبكة العالمية للمعلومات .

ويلاحظ أن هذا التقسيم يتطابق تماما مع التقسيم الفقهي سابق الذّكر للجريمة عبر الكمبيوتر(Cyber Crime) ، وهي في رأيه بأنها" الجرائم التي لها علاقة بالكمبيوتر والشبكة المعلوماتية أو ما تعرف باسم "الويب"، و الانترنت . "**فالويب**"عبارة عن مجموعة كاملة من الوثائق والنصوص والمعلومات والصور والصوت والفيديو وهي ذات شكل تشعبي مرتبط على مستوى العالم، أما **الانترنت** فهي آلية نقل المعلومات عن طريق البروتوكولات الخاصة بالاتصال السلكي و اللاسلكي [2]. وانطلاقا من ذلك قام بتقسيمها إلى أربعة أنواع :

النوع الأول :جرائم الكمبيوتر (Computer Crime) وهي سلوك إنساني يشكل فعلا غير مشروع قانونا ويقع على أجهزة الكمبيوتر سواء وقع هذا السلوك غير المشروع على المكونات المادية (Hard Ware) أو المكونات المعنوية (Soft Ware) أو قواعد البيانات الرئيسية(Data Base)، ومن أمثلتها التخريب لمكونات الكمبيوتر المادية كالشاشات أو الطابعة أو وسائط التخزين المرنة أو الصلبة، وكذلك الفيروسات وتعديل أو محو البيانات الرئيسية وغيرها .

النوع الثاني: جرائم الشبكة العالمية (Web Computer Crime) وهي أيّ سلوك إنساني يكوّن فعلا غير مشروع قانونا ويقع على أيّ وثيقة أو نصّ موجود بالشبكة، ومن أمثلتها قرصنة المعلومات وسرقة أرقام بطاقات الائتمان وانتهاك الملكية الفكرية للبرامج والأفلام وغيرها، فهذه الجرائم تتطلّب اتصالا بالانترنت على عكس جرائم الكمبيوتر التي قد يتصوّر حدوثها سواء كان هناك اتصال بالانترنت أو لا [3].

---

[1] للدكتور ممدوح عبد الحميد عبد المطلب، في مؤلفه ــ البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت، المرجع السابق، ص 88 .

[2] د/ ممدوح عبد الحميد عبد المطلب ، نفس المرجع، 2006 ، ص 18 .

[3] د/ ممدوح عبد الحميد عبد المطلب ، نفس الموضع .

النوع الثالث: جرائم الانترنت (Internet Crime) وهي سلوك إنساني يشكل فعلا غير مشروع قانونا وتقع على آلية نقل المعلومات بين مستخدمي الشبكة العالمية للمعلومات. ومن أمثلة هذه الجرائم جرائم الدخول غير المشروع لمواقع غير مصرح بها للدخول إليها واستخدام عناوين IP غير حقيقية أو زائفة للولوج إلى الشبكة العالمية للمعلومات، كسر البروكسي (Broxey) أو تقنية الحماية (Fire Wall) الخاصة بالجهات المتصلة بالشبكة ..وغيرها .

النوع الرابع : جرائم باستخدام الكمبيوتر (Computer relater Crime)، لا يعتبر استخدام الكمبيوتر أو الشبكة العالمية للمعلومات أو الانترنت في هذه الجرائم من طبيعة الفعل الجرمي، بل تستخدم كوسيلة مساعدة لارتكاب الجريمة، مثل عمليات غسل الأموال، أو نقل المخدرات من مكان لآخر.. ، إلا أن جهاز الكمبيوتر في هذه الحالة يظل محتفظا بآثار رقمية يمكن أن تستخدم للإرشاد عن الفاعل.

هذا التقسيم للدليل الالكتروني وإن كان يتناسب مع تقسيم الفقيه للجرائم عبر الكمبيوتر إلاّ انه لا يتناسب مع مفهوم التقنية الحديثة، فهذه التقسيمات تدور حول موضوع واحد ألا وهو الدليل الالكتروني الخاص بجهاز الكمبيوتر وشبكاته.إلا أنها ميّزت بين شبكات الكمبيوتر والانترنت وبروتوكول تبادل المعلومات والشبكة العالمية للمعلومات التي هي في الأصل واحد، فاختلاف المصطلحات لا يعني اختلافا في المعنى.

ثانيا ـ محاولات الجهات الرسمية لتقسيم الدليل الالكتروني: تعدّ الولايات المتحدة الأمريكية أحسن نموذج فيما يتعلق بالتصدي للجرائم الالكترونية، فهي ثاني دولة بعد السويد في إصدار قوانين خاصة بها تجرّم هذا النوع المستحدث من الإجرام[1]، سواء فيما يتعلق بالولايات المتحدة كدولة أو بالولايات الأعضاء فيها كما هو الحال في ولاية تكساس .. [2]، ومن أهم هذه التشريعات قانون تقرير الأشخاص الصادر في 1970، أيضا قانون الخصوصية الصادر في 31 ديسمبر عام 1974، وقانون حرية المعلومات لعام 1976، وقانون خصوصية الاتصالات سنة 1986، و قانون أخلاق الاتصالات لسنة 1996 ... .

---

[1] تعد السويد من أوائل الدول التي اتجهت إلى سنّ تشريعات قانونية جديدة لمكافحة الإجرام الالكتروني، حيث صدرت أول قانون خاص بها سمي بقانون " البيانات " وذلك في سنة 1973، وقد عالج هذا القانون قضايا الاحتيال عن طريق الانترنت بالإضافة إلى جرائم الدخول غير المشروع على البيانات الالكترونية وتزوير هذه المعلومات، وتحويلها و الحصول غير المشروع عليها . انظر : منير محمد الجنبيهي و ممدوح محمد الجنبيهي، المرجع السابق ، 102 .

[2] د / أحمد خليفة الملط ، الجرائم المعلوماتية ـــ دراسة مقارنة ـــ دار الفكر الجامعي ، 2005 ، ص 173.

وسنحاول فيما يلي عرض تقسيمات وزارة العدل الأمريكية للدليل الالكتروني لسنة 2002، حيث تمّ تقسيمه إلى ثلاث مجموعات وهي كالتالي [1]:

1 ـ السجلات المحفوظة في الحاسوب وهي الوثائق المكتوبة والمحفوظة مثل البريد الالكتروني وملفات برامج معالجة الكلمات ورسائل غرف المحادثة على الانترنت .

2 ـ السجلات التي تمّ حفظ جزء منها إنشاؤها بواسطة الحاسوب، وتعتبر مخرجات برامج الحاسوب وبالتالي لم يلمسها الإنسان مثل (Log Files) وسجلات الهاتف وفواتير أجهزة السحب الآلي ATM .

3 ـ السجلات التي تمّ حفظ جزء منها الإدخال وجزء آخر تمّ إنشاءه بواسطة الحاسوب، ومن أمثلتها: أوراق العمل المالية التي تحتوي على مدخلات تمّ تقليمها إلى برامج أوراق لعمل مثل Excel، ومن تمّ تمّت معالجتها بإجراء العمليات الحسابية عليها .

وهو نفس التقسيم الذي أخذ به القضاء الأمريكي، فسجلات الحاسوب (Computer Records) المقبولة استثناء أمام القضاء الأمريكي إذا كانت معدة في هيئة نصوص Text تتخذ أحد هذه الأشكال: **سجلات الحاسوب المتوالدة (Computer-generated records) وسجلات الحاسوب المخزنة(Computer-stored records)**، والفرق بينهما يتوقف على ما إذا كان الشخص أو الآلة تنشئ محتويات هذه السجلات أي(مصدر هذه السجلات)، فسجلات الحاسوب المخزنة تشير إلى الوثائق التي تحتوي على كتابات (Writings) شخص أو بعض الأشخاص وحدث وان صارت في شكل الكتروني، مثل رسائل البريد الالكتروني (E-mail messages) . أما سجلات الحاسوب المتوالدة فالكمبيوتر هو الذي يصدرها، وهي تحتوي على مخرجات (Output) برامج الحاسوب التي لم تمسّها أيد البشرية مثل سجلات الدخول على الانترنت Log-in records ومصدرها مزود خدمة الانترنت، فهذه السجلات لا تحتوي على بيانات بشرية، فهي مجرد مخرجات كان لابد من جود مدخلات (Input) لها ممثلة في لوغاريتمات البرمجة [2].

---

[1] انظر: د/ سلطان محيا الديحاني ، الجرائم المعلوماتية،على الموقع التالي :
http://www.atsdp.com/forum/zbmszjg-zbgbjgzkni-4377.html

[2] Department of Justice in United States،" Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" July 2002 ،available at:
http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm

ـ وانظر أيضا في نفس المعنى: د/ عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي ، المرجع السابق ، ص 420 و ما بعدها . كذلك انظر لنفس الدكتور، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق ، ص 981 .==

وهناك نوع ثالث من السجلات يجمع بين التدخل الإنساني و معالجة الكمبيوتر، كما لو أدخل متهم بيانات معينة وطلب من الكمبيوتر أن يقوم بمعالجتها توصلا إلى نتائج يسمح بها البرنامج المستخدم، كمن يتهرب من الضرائب فيقوم بتسجيل بيانات غير صحيحة عن دخله وربحه طالبا من الكمبيوتر حساب الضريبة المستحقة [1]. ونشير أن هذه الطبيعة الخاصة بكل نوع تنعكس على قيمته الاثباتية، فهي ليست على درجة واحدة من القوة و القبول أمام المحاكم الأمريكية [2] .

ويؤخذ على هذه التقسيمات أنّها ليست شاملة للدليل الالكتروني بل اقتصرت على نوع محدد منه، وهي سجلات الحاسوب التي تحتوي على نص، بالرغم من أن الدليل الرقمي يشمل كافة البيانات الرقمية الممكن تداولها رقميا كالصور والأصوات والرسوم وغيرها، بل تستخدم حاليا بروتوكولات الاتصالات والتطبيقات المعلوماتية في تحقيق الجرائم الالكترونية، ويعتبر نظام (TCP/IP)[3] من أكثر البروتوكولات المستخدمة في شبكات الإنترنت فهي جزء أساسي منه، حيث تدل بصفة جازمة عن مصدر الجهاز المستخدم في الجريمة وتحدّد الأجهزة التي أصابها الضرر من الفعل الإجرامي وتحديد نوعية النشاط الإجرامي خلال الفترة الزمنية لاقتراف الجريمة.

من خلال هذا العرض، نشير إلى أنّ أيّة محاولة لتقسيم الدليل الالكتروني ينبغي أن يراعى فيها اعتبار مهم ألا وهو التطور المستمر الذي يطرأ على البيئة الرقمية التي يعيش فيها الدليل الرقمي، ممّا تجعله من الأدلة المتطورة بطبيعتها، فتطور هذه البيئة يكاد يكون تلقائيا هنا، حيث تتسع لإمكانية شمول مظاهر رقمية جديدة، لاسيما وانّ العالم الافتراضي لا

== **اللوغاريتمات أو الخوارزميات** هي مجموعة من التعليمات التي ممكن أن تتبع لانجاز عمل ما بعدد محدد من الخطوات وذلك عبر تجزئة المسألة البرمجية المراد حلها إلى أجزاء صغيرة بسيطة و بتجميع هذه الأجزاء يمكن التوصل إلى الحل الصحيح . انظر: د/ ممدوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت ، المرجع السابق ، ص91 .

(1) د/ شيماء عبد الغني محمد عطا الله ، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة ،2007، ص 409.

(2) انظر فيما سيأتي في الفصل الثاني، ص 130 .

(3) بروتوكول التحكم بالنقل ـــ بروتوكول الانترنت (TCP/IP): هي عائلة بروتوكولات الاتصالات بين عدة أجهزة من الكمبيوتر طورت أساسا لنقل البيانات بين أنظمة (UNIX) ثم أصبحت المقياس المستخدم لنقل البيانات الرقمية عبر شبكة الانترنت بواسطة الاتصال الهاتفي وهما في الأصل بروتوكولين مستقلين في شبكة الانترنت، ويعملان معا وبشكل متزامن حيث يرتكزان على تقنية التبديل المعلوماتي بواسطة الحزم المعلوماتية (Packet) بين مختلف الوصلات السلكية و اللاسلكية المتخصصة التي تربط الشبكات المختلفة الموصلة فيما بينها. لمزيد من التفاصيل بروتوكول (TCP/IP)، انظر: د/ ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP / IP) في بحث وتحقيق الجرائم على الكمبيوتر ،المؤتمر السابق الذكر.

يزال في بداياته ولم يصل بعد إلى منتهاه. فالعالم الرقمي لا ينتهي ولن يكون من السهولة احتوائه، فهو عالم متسع لأبعد مما قد ينتجه الخيال من أفكار حول الحدود [1].

وتجدر الإشارة إلى أنّ هذا التنوع في الدليل الرقمي يفيد بالضرورة انّه ليس هناك وسيلة واحدة للحصول عليه، وإنما تتعدّد هذه الوسائل، وفي كل الأحوال يظلّ الدّليل المستمدّ منه رقميا، حتّى وإن اتخذ هيئة أخرى، ففي هذه الحالة وان اعترف القانون بهذه الهيئة الأخرى فانّ ذلك يكون مؤسسا على **طابع افتراضي** مبناه أهمية الدليل الرقمي ذاته وضرورته، إلاّ انّه لكي يحدث تواصل بين القانون وبين هذا الدليل ـــ نتيجة لنقص توافر الإمكانيات الرقمية في المحاكم ـــ **فانه يلزم اتخاذ مسلك الافتراض من حيث اعتباره دليلا أصليا** [2].

---

[1] د / عمر محمد ابوبكر بن يونس ،الجرائم الناشئة عن استخدام الانترنت ، المرجع السابق ، ص 980.

[2] د / عمر محمد بن يونس، مذكرات في الإثبات الجنائي عبر الانترنت، ندوة الدليل الرقمي بمقر جامعة الدول العربية بجمهورية مصر العربية، في الفترة من 5 ـــ 8 مارس 2006، ص12. مشار إليه عند: عبد الناصر محمد محمود فرغلي ، د / عبيد سيف سعيد المسماري ، المرجع السابق ، ص 14 .

المبحث الثاني
إجراءات جمع الدليل الالكتروني

ممّا لا شك فيه أنّه لا يوجد ما يسمّى بالجريمة الكاملة مهما حاول الجاني إخفاءها، وذلك استنادا إلى قاعدة " **لوكارد لتبادل المواد**" التّي تنص على أنّه عند احتكاك جسمين بعضهما ببعض فانّه لابّد وأن ينتقل جزء من الجسم الأوّل إلى الثاني و بالعكس[1]، وبالتالي ينتج عن هذا الاحتكاك ما يعرف بالدليل الجنائي، وفي مجال الجريمة الالكترونيّة لدينا الدليل الالكتروني، وحتّى يتحقّق هذا الدليل لإثبات هذا النوع المستحدث من الإجرام، فإنّه لابد من جمع عناصر التحقيق والدعوى، وتقديم هذه العناصر إلى سلطة التحقيق الابتدائي، فإذا أسفر هذا التحقيق عن دليل أو ترجّح معها إدانة المتّهم قدمته إلى المحكمة، ومرحلة المحاكمة هي أهمّ المراحل لأنها مرحلة الجزم بتوافر دليل أو أدلة يقتنع بها القاضي لإدانة المتهم وإلا قضي ببراءته.

إلا أنّ خصوصيّة الجريمة الالكترونيّة وذاتيّة الدليل الالكتروني سيقودان دون شك إلى تغيير، كبير إن لم يكنا كليّا في المفاهيم السائدة حول إجراءات الحصول على هذا الدليل، وذلك نتيجة لضآلة دور بعض الإجراءات التقليديّة في بيئة تكنولوجيا المعلومات كالمعاينة أو الشهادة مثلا، وبالتالي يقودنا إلى إتباع نوع مستحدث من الإجراءات يتلاءم وطبيعة هذه البيئة .

وعلى ذلك سنتناول في هذا المبحث الإجراءات التقليدية لجمع الدليل الالكتروني أوّلا، ثم يليه الإجراءات الحديثة لجمع هذا الدليل.

---

[1] د/ خالد حمد محمد الحمادي، المرجع السابق، ص 19.

المطلب الأول
الإجراءات التقليديّة لجمع الدليل الالكتروني

نظّم المشرع كيفية استنباط الدليل عن طريق إجراءات تتبع وصولا إلى هذه الغاية، وأهم هذه الإجراءات كما بيّنها القانون، هي المعاينة والتفتيش، وضبط الأشياء، سماع الشهود وندب الخبراء، وهي تستخدم بصفة عامة لجمع الدليل في جميع الجرائم التقليديّة منها والمستحدثة، إلا أن دورها يكون بين المدّ في الجرائم الأولى والجزر في الثانيّة، وهو ما سوف نلاحظه في الفروع المتقدّمة من هذا المطلب.

الفرع الأول
الإجراءات الماديّة

سنتناول في هذا الفرع ثلاث إجراءات وهي المعاينة ،والتفتيش والضبط وهي إجراءات ذات طبيعة ماديّة، حيث تتم في الغالب نتائج ماديّة ملموسة، وسوف نبيّن في التالي دور كل إجراء في استنباط الدليل الالكتروني.

أولاً: المعاينة

أ ـ فكرة عامة عن المعاينة التقنية لمسرح الجريمة الالكترونية :عرّف جانب من الفقه[1] المعاينة بأنّها " رؤية بالعين لمكان أو شخص أو شيء لإثبات حالته وضبط كلّ ما يلزم لكشف الحقيقة"، وقد عرّفها البعض[2] بأنها" إجراء بمقتضاه ينتقل المحقّق إلى مكان وقوع الجريمة ليشاهد بنفسه ويجمع الآثار المتعلّقة بالجريمة وكيفية وقوعها وكذلك جمع الأشياء الأخرى التّي تفيد في كشف الحقيقة". وأيّا كان التعريف الموضوع لها فهي تتطلّب سرعة الانتقال إلى محلّ الواقعة الإجرامية لمباشرتها وذلك لإثبات حالته و ضبط الأشياء التي تفيد في إثبات وقوعها ونسبتها إلى فاعلها. وقد نصّت على المعاينة في مرحلة جمع الاستدلالات المادة(1/24) من قانون الإجراءات الجنائية المصري، ونصّت عليها المادة (31/ 1) من ذات القانون، وذلك في إطار حصر مهام وواجبات مأمور الضبط القضائي في الأحوال العادية وفي حالات التلبس [3].

---

[1] د/ محمد زكي أبو عامر، الإجراءات الجنائيّة، دار الجامعة الجديدة، الإسكندرية، الطبعة السابعة، 2002، ص 233.

[2] د/ مأمون محمد سلامة، الإجراءات الجنائية في التشريع المصري، المرجع السابق، ص 642 وما بعدها .

[3] تنص المادة (1/24) من قانون الإجراءات الجنائية المصري:" يجب على مأموري الضبط القضائي أن يقبلوا التبليغات والشكاوى التي ترد إليهم بشأن الجرائم ...ويجب عليهم وعلى مرؤوسيهم أن يحصلوا على==

والأصل في المعاينة أنّها إجراء من إجراءات التحقيق[1]، ولذلك ففي غير حالات التلبّس التي نصّ عليها القانون يلزم أن تقوم بها سلطة التحقيق بنفسها أو تنتدب مأمور الضبط للقيام بها [2]، ويقتضي ذلك تحرير محضر بها عن طريق كاتب، لأنّها من الإجراءات التّي تستلزم من المحقق تفرغا ذهنيا [3]، وتتّبع في شأنها أيضا جميع القواعد التّي تحكم إجراءات المحاكمة، من إخطار الخصوم بمكان المعاينة وزمانها ليتمكّنوا من الحضور أثناء إجراءها[4]. كما يمكن للمحكمة أن تقوم بإجراء المعاينة إذا ما رأت في ذلك سبيلا في كشف الحقيقة، سواء كان ذلك من تلقاء نفسها أو بناء على طلب الخصوم[5]. أمّا في فرنسا فيمكن إجراء المعاينة عن طريق المحضر أو الخبير بناء على طلب الشخص المعني بعد موافقة القاضي المختص بناء على طلب على عريضة، خاصّة إذا كان المكان الذي تجرى فيه المعاينة خاصّا، حتى ولو كان مفتوحا للجمهور[6].

هذا فيما يخص بالأحكام العامة للمعاينة، وسنتناول فيما يلي المعاينة في الجريمة الالكترونية، ومدى أهميتها مقارنة بالجريمة التقليدية، وما هي القواعد الواجب اتخاذها حتّى تأتي المعاينة بثمارها وتفي بأغراضها المنشودة ؟.

==جميع الإيضاحات و **يجروا المعاينات اللازمة لتسهيل تحقيق الوقائع** التي تبلغ إليهم أو التي يعلنون بها بأي كيفية كانت..". أما المادة (1/31) من ذات القانون فتنص على: " يجب على مأمور الضبط القضائي في حالة التلبس بجناية أو جنحة **أن ينتقل فورا إلى محل الواقعة ويعاين الآثار المادية للجريمة و يحافظ عليها، ويثبت حالة الأشخاص وكل ما يفيد في كشف الحقيقة** ويسمع أقوال من كان حاضرا، أو من يمكن الحصول منه على إيضاحات في شأن الواقعة ومرتكبيها". ويقابل ذلك **المادة(42)** من قانون الإجراءات الجزائية الجزائري .

(1) تنص المادة (90) من قانون الإجراءات الجنائية المصري على: "ينتقل قاضي التحقيق إلى أيّ مكان كلما رأى ذلك ليثبت حالة الأمكنة و الأشياء و الأشخاص ووجود الجريمة ماديّا وكل ما يلزم إثبات حالته"، ويقابل ذلك المادة (79) من قانون الإجراءات الجزائية الجزائري حيث تنص على:" يجوز لقاضي التحقيق الانتقال إلى أماكن وقوع الجرائم لإجراء جميع المعاينات اللازمة أو للقيام بتفتيشها. ويخطر بذلك وكيل الجمهورية الذي له الحق في مرافقته. ويستعين قاضي التحقيق دائما بكاتب التحقيق و يحرّر محضر بما يقوم به من إجراءات ".

(2) د/ محمد علي الحمال، التقاط الدليل المادي من مسرح الجريمة، مجلة كلية الدراسات العليا، العدد الثاني، يناير 2000، ص 190.

(3) نقض 8 مايو سنة 1961، مجموعة أحكام النقض، س 12رقم 101، ص541.

(4) د/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار الفكر العربي، القاهرة، 2001، ص27.

(5) د/ جلال ثروت, نظم الإجراءات الجنائيّة, دار الجامعة الجديدة للنشر, الاسكندرية, 1997, ص 456.

(6) د/ جميل عبد الباقي الصغير، نفس المرجع، ص27.

للمعاينة أهميّة كبيرة في كشف غموض الكثير من الجرائم التقليدية[1]، فيما عدا حالات استثنائية كما هو الحال في جريمة التزوير المعنوية وجريمة السب التي تقع بالقول في غير علانية [2]، إلاّ أنّ دورها في مجال كشف غموض الجريمة الالكترونية وضبط الأشياء التي قد تفيد في إثبات وقوعها ونسبتها إلى مرتكبيها لا ترق إلى نفس الدرجة من الأهمية، ومردّ ذلك إلى الاعتبارات الآتية [3]:

1– إنّ الجرائم الالكترونية قلّما يتخلف عن ارتكابها آثارا مادية، فما ينتج عنها من أدلّة ما هو إلاّ بيانات غير مرئية.

2 – تردّد العديد من الأشخاص على مسرح الجريمة خلال الفترة الزمنية الطويلة بين ارتكابها واكتشافها ممّا يفسح المجال لحدوث إتلاف أو تغيير أو عبث بالآثار الماديّة، ممّا يدخل الشكّ على الدليل المستمّد من المعاينة.

3 – إمكانيّة تلاعب الجاني في البيانات عن بعد أو محوها عن طريق التدخل من خلال وحدة طرفية، لذلك ينبغي على المشرّع أن يقرّر جزاءات جنائية على كلّ من يقوم بإجراء أيّ تغيير أو تعديل في المعلومات المسجّلة في ذاكرة الحاسوب أو وسائط التخزين أو في بنك المعلومات أو قاعدة البيانات، قبل قيام سلطة التحقيق بإجراء المعاينة، وهو ما نصّ عليه كلٌ من المشرع الجزائري في المادة (43) من قانون الإجراءات الجزائية الجزائري[4] والمشرع الفرنسي من خلال المادة (1/55) من قانون الإجراءات الجنائية الفرنسي[5]، وذلك حرصا منهما على المحافظة على مسرح الجريمة قبل القيام بالإجراءات الأولية للتحقيق الجنائي، والملاحظ أنّ

---

[1] لمزيد من التفصيل حول أهمية المعاينة، انظر: د/ محمد محمد محمد عنب، معاينة مسرح الجريمة، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، 1988، ص 13. وانظر أيضا: د سعد أحمد محمود سلامة, مسرح الجريمة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2007، ص 30.

[2] د/ هشام محمد فريد رستم، الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994، ص 57– 58 .

[3] د/ هشام محمد فريد رستم، نفس المرجع ، ص 59 .

[4] تنص المادة (43) من قانون الإجراءات الجزائية الجزائري : " يحظر في مكان ارتكاب جناية على كل شخص لا صفة له، أن يقوم بإجراء أي تغيير على حالة الأماكن التي وقعت فيها الجريمة أو ينزع أي شيء منها قبل الإجراءات الأولية للتحقيق القضائي، و إلاّ عوقب بغرامة 200 إلى 1000دج.

غير أنه يستثنى من هذا الحظر حالة ما إذا كانت التغييرات أو نزع الأشياء للسلامة و الصحة العمومية أو تستلزمها معالجة المجني عليهم.

وإذا كان المقصود من طمس الآثار أو نزع الأشياء هو عرقلة سير العدالة عوقب على هذا الفعل بالحبس من ثلاثة أشهر إلى ثلاثة سنوات و بغرامة من 1.000الى 10.000 دج".

[5] Article 55 du C.P.P.F, dispose que :" Dans les lieux où un crime a été commis‹ il est interdit, sous peine de l'amende prévue pour les contraventions de la 4° classe, à toute personne non habilitée, de modifier avant les premières opérations de l'enquête judiciaire l'état des lieux et d'y effectuer des prélévement quelconques ".

أحكام هذه النصوص وان كانت تنصرف إلى اغلب الجرائم التقليدية، إلاّ أنّه يمكن تطبيقها عند معاينة مكوّنات الحاسوب ذات الطابع المادي كأشرطة الحاسوب وكابلاته وشاشة العرض الخاصة به والأقراص وغيرها، بخلاف معاينة المكونات غير المادية لأنها تتطلّب إجراءات خاصة [1].

3 ـ مشكلة تبخّر الدليل الالكتروني الذي يمكن تعديله أو تغييره أو محوه في بضع ثواني. لذلك أجاز المشرع الأمريكي لعضو النيابة العامة أن يعجّل بإجراء المعاينة خشية ضياع الأدلة وذلك بإرسال رسالة إلى مزوّد خدمة الإنترنت يلزمه فيها بتتبّع السجّلات المطلوبة إلى حين صدور أمر المحكمة باتّخاذ هذا الإجراء أو غيره [2].

ونظرا لما تتميّز به الجريمة الالكترونية من خصائص، فبإمكان المحقق أو مأمور الضبط القضائي أن يستعين بالخبراء للفحص وإبداء الرأي الفنّي في الأمور التي تستعصى على هؤلاء فهمها وتفسيرها وذلك حتّى يمنع أيّ تشكيك في صحة الدليل المستمد منه.

وتتخذ المعاينة في الجرائم الالكترونية عدّة أشكال وذلك حسب نوعية الجريمة المرتكبة، ففي جرائم العدوان على الملكية الفكرية يتمّ إنزال نسخة من المصنّف المعتدى عليه أو التحفظ على نسخة منه وذلك بطباعتها و استخراجها في هيئة ورقية أو صلبة، وحديثا تستعمل تقنية الطباعة على خشب أو بلاستيك خاص، إلاّ أنّ هناك طرقا عامة تتوافق مع طبيعة النظام المعلوماتي، مثل وسيلة تصوير شاشة الحاسوب (Impression de captures d'écran) وذلك بواسطة آلة تصوير تقليدية أو عن طريق استخدام برمجية حاسوب متخصصة في أخذ صورة لما يظهر على الشاشة، وهو ما يعرف بـ " طريقة تجميد مخرجات الشاشة "Frozen أو أن يكون ذلك عن طريق حفظ الموقع باستخدام خاصية الحفظ (Save as) المتوافرة في نظام التشغيل.

ب ـ كيفية إجراء المعاينة التقنيّة لمسرح الجريمة الالكترونية: عند العلم بوقوع الجريمة فانّ أوّل خطوة يقوم بها مأمور الضبط القضائي هو الانتقال إلى مسرح الجريمة، لانّ هذا الأخير حجر الزاوية في التحقيق الجنائي ومكمّن الآثار والأدلّة المادية، وينبغي التعامل في هذا الإطار مع مسرح الجريمة الالكترونية على أنّه مسرحان هما:

ـ مسرح تقليدي: ويقع خارج بيئة الحاسوب والانترنت، ويتكوّن بشكل رئيسي من المكونات الماديّة المحسوسة للمكان الذي وقعت فيه الجريمة، وهو أقرب ما يكون إلى مسرح أيّة جريمة

---

[1] انظر فيما سيأتي ص51.

[2] Daniel Morris-Tracking a computer Hacker US Attorneys bulletin 2/2001 p. 3. . gov/criminal/ cybercrime USA may 2001 htm.www.U.S.Aavailable at:

تقليدية، قد يترك فيها الجاني آثار عدّة، كالبصمات وبعض متعلقاته الشخصيّة او وسائط تخزين رقميّة.

– **مسرح افتراضي:** ويقع داخل البيئة الالكترونيّة، ويتكوّن من البيانات الرقميّة التي تتواجد داخل الحاسوب وشبكة الانترنت، في ذاكرة الأقراص الصلبة الموجودة بداخله.

وإذا كانت عمليّة الانتقال إلى المسرح التقليدي تتمّ بطريقة مادية، فالأمر يختلف بالنسبة إلى المسرح الافتراضي، فلا يكون بالضرورة عبر العالم المادي، وإنّما عبر العالم الافتراضي، حيث يستطيع عضو سلطة التحقيق أو مأمور الضبط القضائي أن يقوم بهذه المعاينة وهو جالس في مكتبه من خلال الحاسوب الموضوع في المحكمة، كما يمكنه أن يلجأ إلى بيت الخبرة القضائية أو إلى الخبرة الاستشارية أو إلى مقهى الانترنت، ويمكنه اللجوء أيضا إلى مقر مزود الانترنت الذي يعدّ أفضل مكان يمكن من خلاله إجراء المعاينة [1].

ونتيجة لاختلاف مسرح الجريمة الالكترونية عن غيره من الجرائم لكون هذا النوع من الجرائم يتميّز بوجود الأدلة الالكترونية ذات الطبيعة غير المرئية، لذلك ينبغي تعامل خاص معه ويكون ذلك من خلال إتّباع عدّة قواعد فنيّة قبل الانتقال إلى مسرح الجريمة الالكترونية أبرزها ما يلي :

1 – توفير معلومات مسبقة عن مكان الجريمة، نوع وعدد الأجهزة المتوقّع مداهمتها و شبكات الاتصال الخاصّة بها .

2 – إعداد خريطة للموقع الذي تتمّ الإغارة عليه، وإعداد خطة للهجوم على ذلك المكان وتكون موضحة بالرسومات .

3 – إعداد فريق التفتيش من المتخصّصين، على أن يكون هذا الفريق مرفقا بالأمر القضائي اللازم للقيام بالتفتيش، لان اغلب الجرائم الالكترونية تكون داخل أمكنة لها خصوصياتها [2].

4 – الحصول على الاحتياجات الضرورية من أجهزة وبرامج للاستعانة بها في الفحص والتشغيل مثل برنامج معالجة الملفات (Xtree Pro Gold)، وبرنامج النسخ(Lap Link)، وبرنامج (Encase) الذي ينتج صورا مطابقة من القرص الصلب، ويستخدم بصفة خاصة لأغراض التحقيقات الجنائية في المباحث الفدراليّة الأمريكيّة ويسميها الخبراء " حقيبة الأدلة الرقمية".

---

[1] د / عمر أبوبكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق، ص 895 .

[2] د/ محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي والانترنت، المرجع السابق، ص 357.

5 ــ تأمين التيّار الكهربائي من الانقطاع المفاجئ، لأنّ ذلك بسبب العديد من المخاطر تتمثل في محو المعلومات من الذاكرة من جراء غلق جهاز الكمبيوتر، وبالتالي فقدان كافة العمليّات التي كان يتمّ تشغيلها واتصالات الشبكة وأنظمة الملفات الثابتة [1].

ومن الإجراءات التّي يتعيّن إتباعها عند إجراء المعاينة ما يلي:

1 ــ القيام بتصوير جهاز الحاسب الآلي الذّي ترتكب عن طريقه الجرائم وما قد يتّصل به من أجهزة طرفية و محتوياته وأوضاع المكان الذي يوجد به بصفة عامة مع العناية بتصوير أجزاءه الخلفية وملحقاته الأخرى[2].

2 ــ العناية البالغة بملاحظة الطريقة التّي تمّ بها إعداد النظام، والآثار الالكترونية التي يخلّفها ولوج النظام أو التردّد على المواقع بشبكة المعلومات، وبوجه خاص السجلات الالكترونية التي تزود بها شبكات المعلومات لمعرفة موقع الاتصال ونوع الجهاز الذي تمّ عن طريقه الولوج إلى النظام أو الموقع أو الدخول معه في حوار[3].

3 ــ عدم التسرّع في نقل أيّ مادة معلوماتية من مكان وقوع الجريمة وذلك قبل إجراء الاختبارات اللازمة للتيقّن من عدم وجود أيّ مجالات مغناطيسية في المحيط الخارجي حتّى لا يحدث أيّ إتلاف للبيانات المخزّنة.

4 ــ القيام بحفظ المستندات الخاصة بالإدخال وكذلك مخرجات الحاسوب الورقيّة ذات الصلة بالجريمة ورفع ما قد يوجد عليها من بصمات أو آثار ماديّة.

5 ــ ربط الأقراص الكومبيوترية التي ربما تحمل الأدلة، مع جهاز يمنع الكتابة أو التسجيل عليها، ممّا يتيح للمحققين قراءة بياناتها من دون تغييرها [4].

5 ــ التحفظ على محتويات سلّة المهملات، والقيام بفحص الأوراق والشرائط والأقراص الممغنطة المحطّمة المتواجدة فيها، ورفع البصمات التي قد تكون لها صلة بالجريمة المرتكبة.

6 ــ الاستعانة بأهل الخبرة عند الضرورة .

---

[1] قد لا يكون فقدان هذا الدليل أمرا هام عند التعامل مع أجهزة الكمبيوتر الشخصية (Personal Computer) حيث يمكن تخزين المعلومات في الذاكرة العشوائية (Ram Slack) أو في الذاكرة الظاهرة (Virtual Memory) في شكل ملفات (Swap and Page Files). انظر: د/ ممدوح عبد الحميد عبد المطلب، البحث و التحقيق الجنائي الرقمي، المرجع السابق، ص 115 .

[2] د /هشام محمد فريد رستم ، الجوانب الإجرائية للجرائم المعلوماتية ، المرجع السابق ص 60 .

[3] د/ سليمان أحمد فاضل، المواجهة التشريعيّة والأمنيّة للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت) ، دار النهضة العربية، القاهرة، 2007، ص290. وانظر أيضا: د/ عبد الفتاح بيومي حجازي، مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الطبعة الأولى، 2006، الإسكندرية، ص 104.

[4] لمزيد من التفاصيل انظر الموقع التالي :

http://www.paldf.net/forum/showthread.php?t=219932

ثانيا: التفتيش في البيئة الالكترونية

التفتيش[1] إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة في مستودع السر، لذلك يعتبر من أهمّ إجراءات التحقيق في كشف الحقيقة لأنّه غالبا ما يسفر عن أدلّة مادية تؤيد نسبة الجريمة إلى المتهم.

والتفتيش ليس غاية في حدّ ذاته، وإنّما هو وسيلة لغاية تتمثّل فيما يمكن الوصول من خلاله إلى أدلّة ماديّة تسهم في بيان وظهور الحقيقة [2]. ونتيجة لذلك يعدّ تفتيش نظام الحاسوب والانترنت من أخطر المراحل حال اتخاذ الإجراءات الجنائية ضد مرتكب الجريمة الالكترونية، لكون محلّ التفتيش هنا ـــ وهو الحاسوب والشبكات ـــ محلّ جدل فقهي متزايد يوما بعد يوم خاصة بالنسبة للكيان المعنوي للحاسوب فهو مجرد برامج وبيانات الكترونية ليس لها أيّ مظهر مادي محسوس. **فما مدى صلاحية مكونات و شبكات الحاسوب كمحلّ يرد عليه التفتيش، و ما هي الضوابط التي يجب إتباعها في ذلك؟** وهذا ما سوف نتناوله على النحو التالي:

1 ـ مدى قابلية مكوّنات وشبكات الحاسوب للتفتيش:

تتكوّن نظم الحاسوب من مكوّنات ماديّة(Hardware) ومكوّنات منطقيّة (Software)، كما أنّه تربطه بغيره من الحاسبات شبكات اتصال بعدية[3] على المستوى المحلّي أو الدولي.

أ ـ تفتيش مكوّنات الحاسوب الماديّة:

الواقع أنّ تفتيش المكوّنات الماديّة للحاسوب بأوعيّتها المختلفة بحثا عن شيء يتّصل بجريمة الكترونيّة وقعت ويفيد في كشف الحقيقة عنها وعن مرتكبيها، يدخل في نطاق التفتيش طالما تمّ وفقا للإجراءات القانونية المقرّرة، بمعنى أنّ حكم تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، سواء من الأماكن العامة أو الأماكن الخاصة، إذ أنّ لصفة المكان أهميّة خاصّة في مجال التفتيش، فإذا كانت موجودة في مكان خاص كمسكن المتّهم أو أحد ملحقاته كان لها حكمه،

---

[1] يقصد بالتفتيش"إجراء من إجراءات التحقيق يقوم به موظّف مختص، طبقا للإجراءات المقررة قانونا، في محلّ يتمتّع بحرمة، بهدف الوصول إلى أدلة مادية لجناية أو جنحة تحقّق وقوعها لإثبات ارتكابها أو نسبتها إلى المتّهم ". لمزيد من تعريفات أخرى للتفتيش انظر: د/ عوض محمد عوض، قانون الإجراءات الجنائي، الجزء الأول، مؤسسة الثقافة الجامعية، 1989، ص 475. د/ محمود محمود مصطفى، الإثبات في المواد الجنائية في القانون المقارن، المرجع السابق، ص 14. وانظر أيضا: د/ أحمد فتحي سرور، المرجع السابق، ص 544. انظر كذلك: د/ قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005، ص 15. وانظر أيضا: أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر، 1999، ص 40.

[2] د/ حسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون المقارن، منشأة المعارف، الإسكندرية، 1982، ص 385.

[3] د/ علاء الدين محمد فهمي وآخرون، د/.محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، القاهرة مطابع المكتب المصري الحديث سنة 1991، ص 10 .

فلا يجوز تفتيشها إلاّ في الحالات التي يجوز فيها تفتيش مسكنه و بنفس الضمانات المقرّرة قانونا في أغلب التشريعات الجنائية كالقانون المصري[1]، إلاّ أنّ القانون الجزائري قد خالف نص (المادة 64) [2] من قانون الإجراءات الجزائية وأورد عليها استثناءات بموجب قانون رقم (06ــ 22) المعدّل و المتمّم للأمر رقم (66 ــ 155) والمتضمن قانون الإجراءات الجزائية، حيث استثنى المشرع تطبيق هذه الضمانات على طائفة من الجرائم المذكورة في (الفقرة الثالثة من المادة 45) [3] من القانون رقم (06ــ 22) ومن بينها الجرائم **الماسة بأنظمة المعالجة الآلية للمعطيات**، حيث نصّ في المادة 64 فقرة الثالثة " غير أنّه عندما يتعلّق الأمر بتحقيق جار في إحدى الجرائم المذكورة في المادة 47 (الفقرة 3) من هذا القانون، تطبّق الأحكام الواردة في تلك المادّة وكذا أحكام المادة (47 مكرّر) حيث أجاز إجراء التفتيش في كلّ محلّ سكني أو غير سكني في كلّ ساعة من ساعات النّهار أو اللّيل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص. والملاحظ أنّ المشرع الجزائري غلّب في هذه الحالة مصلحة المجتمع في تحقيق العدالة على مصلحة الأفراد في حقهم على الحفاظ على حرمتهم الخاصة لاسيما حرمة المسكن باعتبار مستودع أسرارهم، فظاهر النص يشير إلى التعدي(المشروع) على حرمة الحياة الخاصة للشخص، إلاّ أنّ ما يبرره ويقلّ من خطورته الطبيعة الخاصة للجريمة الالكترونيّة، فهي جريمة قابلة للمحو والتعديل في أقل من ثانيّة، ومرتكبها ذو دراية بالأمور التقنيّة، وقد تكون الصعوبة أكثر إذا كان هذا الدليل الالكتروني الوحيد في الدعوى الجنائية، لذلك أجاز المشرع إجراء تفتيش منزل المتهم في حالة واحدة وهي حالة صدور إذن من وكيل الجمهوريّة المختص.

---

[1] يشترط المشرع المصري لصحة تفتيش منزل المتهم صدور الأمر القضائي المسبب ولو في حالة التلبس، وذلك بعد الحكم بعدم دستورية المادة 47 إجراءات جنائية مصري، فضلا عن شروط التفتيش العامة. لمزيد من التفصيل انظر: د/ عوض محمد عوض، المرجع السابق، ص 311 وما بعدها، وانظر أيضا: د/ سامي حسن الحسني، النظرة لعامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1996، ص 163.

[2] تنص **المادة(64)** من قانون الإجراءات الجزائية الجزائري" لا يجوز تفتيش المساكن و معاينتها و ضبط الأشياء المثبتة للتهمة إلاّ برضا صريح من الشخص الذي ستتخذ لديه هذه الإجراءات. و يجب أن يكون هذا الرضا بتصريح مكتوب بخط يد صاحب الشأن، فأن كان لا يعرف الكتابة فبإمكانه الاستعانة بشخص يختاره بنفسه، و يذكر ذلك في المحضر مع الإشارة صراحة إلى رضاه.

وتطبق فضلا عن ذلك أحكام المواد من(44الى 47) من هذا القانون."

[3] تنص (**المادة 3/47 من القانون رقم 06 ــ 22**) على" عندما يتعلّق الأمر بجرائم المخدرات أو الجريمة المنظمة عبر الحدود الوطنيّة أو **الجرائم الماسّة بأنظمة الحاسب** والإرهاب وكذا الجرائم المتعلقة بالتشريع الخاص بالصرف فإنّه يجوز إجراء التفتيش والمعاينة والحجز **في كل محل سكني أو غير سكني في كل ساعة من ساعات النهار أو الليل وذلك بناء على إذن مسبق من وكيل الجمهورية المختص**" .

أما بالنسبة للأماكن العامة، فإذا وجد الشخص في هذه الأماكن وهو يحمل مكوّنات الحاسب سالفة الذّكرأو كان مسيطرا عليها أو حائزا لها فإنّ تفتيشها لا يكون إلاّ في الحالات التي يجوز فيها تفتيش الأشخاص وبنفس الضمانات والقيود المنصوص عليها في هذا المجال.

ب ـ مدى خضوع مكوّنات الحاسوب المعنوية للتفتيش: لقد ثار خلاف تشريعي وفقهي بشأن مدى جواز تفتيش المكوّنات المعنوية للحاسوب تمهيدا لضبط الأدلة الالكترونية .

فذهب الرأي الأوّل إلى جواز تفتيش نظم الحاسوب، ويستند في ذلك إلى عمومية نصوص التفتيش، وذلك من خلال توسيع تفسير عبارة ضبط "**أي شيء**"، لتشمل المكونات الحاسوب المادية وغير المادية. فالمادة (487)عقوبات كندي تقضي بإمكانية إصدار أمر قضائي لتفتيش وضبط أيّ شيء... تتوافر بشأنه أسس ومبررات معقولة تدعو للاعتقاد بأنّ جريمة قد وقعت أو يشتبه في وقوعها، أو أنّ هناك نيّة لاستخدامه في ارتكاب جريمة، أو أنه سينتج دليلا على وقوع الجريمة[1]. وحتّى الآن فإنّ هذا النص يفسر بوضوح تام على أنّه يسمح بتفتيش المكوّنات المعنوية للحاسوب.

وعلى النقيض من ذلك هناك رأي آخر يرى أنّه إذا كانت الغاية من التفتيش هي ضبط الأدلة الماديّة التي تفيد في كشف الحقيقة فإنّ هذا المفهوم المادي لا ينطبق على الأدلة الالكترونية. ففي فرنسا مثلا يرى بعض الفقهاء أنّ النبضات الالكترونية أو الإشارات الالكترونية الممغنطة لا تعدّ من قبيل الأشياء المحسوسة، وبالتالي لا تعتبر شيئا ماديّا بالمعنى المألوف. وقد استجاب المشرع الفرنسي لهذه التغيرات وقام بتعديل نصوص التفتيش بالقانون رقم (**545ـ 2004**) المؤرخ في 21 جوان 2004، حيث قام بإضافة عبارة "**المعطيات المعلوماتية**" في المادة (94) من قانون الإجراءات لتصبح المادة على النحو التالي: " يباشر التفتيش في جميع الأماكن التّي يمكن العثور فيها **على أشياء أو معطيات معلوماتية** يكون كشفها مفيدا لإظهار الحقيقة"[2]. و الملاحظ أنّ ما قام به المشرّع الفرنسي أولى بالإتّباع لاسيما أنّ المشرّع الجزائري جرّم أفعال المساس بأنظمة المعالجة الآلية للمعطيات بموجب القانون رقم (04ــ15 المؤرخ في 10 نوفمبر سنة 2004).

وفي هذا الصدد صرّحت الاتفاقية الأوربية في شأن جرائم السيبر بحق الدول الأعضاء في تفتيش أجهزة الكمبيوتر في إطار الإجراءات الجنائية، وذلك من خلال المادة (19 من القسم

---

[1] د/ هلالي عبد الله أحمد، تفتيش نظم الحاسب الآلي وضمانات المتهم المعلومــاتي، دراســة مقارنـــة، دار النهضة العربيّة، القاهرة، 2006، ص 201.

[2] Article 94 du C.P.P.F, dispose que :" Les perquisitions sont effectuées dans tous les lieux où peuvent se trouver **des objets ou des données informatiques** dont la découverte serait utile à la manifestation de la vérité ".

الرابع) حيث نصّت على" أنّ لكل طرف من حقها أن تسنّ من القوانين ما هو ضروري لتمكين السلطات المختصّة بالتفتيش أو الدخول إلى:

ـ نظام الكمبيوتر أو جزء منه أو المعلومات المخزّنة به.

ـ الوسائط التي يتم تخزين معلومات الكمبيوتر بها ما دامت مخزّنة في إقليمها.

ج ـ مدى خضوع شبكات الحاسوب للتفتيش "التفتيش عن بعد":

إنّ طبيعة التكنولوجيا الرقميّة قد عقّدت من التحدّي أمام أعمال التفتيش والضبط، وذلك بسبب امتداد الأدلة الالكترونيّة عبر شبكات الحاسوب في أماكن بعيدة عن الموقع المادي للتفتيش، وان كان من الممكن الوصول إليها من خلال الحاسوب المأذون بتفتيشه، وقد يكون الموقع الفعلي للبيانات داخل اختصاص قضائي آخر أو حتّى في بلد آخر. فهل يمتد تفتيش حاسوب معيّن إلى الأجهزة المرتبطة به سواء كانت موجودة داخل البلاد أو خارجه؟ يثار التساؤل حول أثر تفتيش الأنظمة المتصلّة بالنظام المأذون بتفتيشه إذا تواجدت في دوائر اختصاص مختلفة.

في هذه الصورة يمكن التفرقة بين الفرضين التاليين:

الفرض الأوّل: اتصال حاسب المتهم بحاسب موجود في مكان آخر داخل الدولة:

ـ وجدت بعض التشريعات المقارنة حلاّ لهذه المشكلة كما في الولايات المتّحدة عندما أجازت التوجيهات الداخلية الخاصة بإجراءات التفتيش أن يمتدّ إذن التفتيش الصادر لمقر شركة معيّنة إلى فروعها الكائنة في نفس العقار[1]. وكذلك الحال بالنسبة لكندا، حيث أصدرت نظاما خاصا بتفتيش الكمبيوتر تضمنه القانون الجنائي الكندي في المادة (subsection 487 (2.1) (a بمقتضى التعديل الصادر في 8 مارس 1996[2].

وقد نصّت المادة 17 فقرة (أ) من القانون الفرنسي رقم(239 لسنة 2003) بشأن الأمن الداخلي الصادر في 18 مارس سنة 2003 بأنّه يمكن لرجال الضبط القضائي أن يدخلوا من الجهاز الرئيسي على البيانات التي تهمّ عملية البحث والتحرّي، فتنصّ المادة 17منه على أنّه" يجوز لرجال الضبط القضائي من درجة ضباط وغيرهم من رجال الضبط القضائي أن يدخلوا عن طريق الأنظمة المعلوماتية المثبتة في الأماكن التي يتمّ فيها التفتيش على البيانات التي تهمّ

---

(1) Verguchi Pascal, la répression de délit informatique dans une perspective international, these, Mootepellier 1996, p. 368.

مشار إليه عند: د/ شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 298.

(2) تنص المادة (subsection 487 (2.1) (a) على أنّه" للقائم بتفتيش النظام وفقا لأحكام هذا الفصل أن يقوم بتفتيش أجهزة الكمبيوتر الأخرى المتواجدة في نفس المكان أوفي نفس المبنى الذي صدر بخصوصه إذن بتفتيش كمبيوتر متواجد فيه لضبط و تفتيش البيانات التي تحتويها تلك الأجهزة أو البيانات المتاحة لهذه الأجهزة".

التحقيق والمخزنة في النظام المذكور أو في أيّ نظام معلوماتي آخر مادامت هذه البيانات متّصلة في شبكة واحدة مع النظام الرئيسي أو يتمّ الدخول إليها أو تكون متاحة ابتداء من النظام الرئيسي"[1].

وتسمح الاتفاقية الأوربية لجرائم الانترنت لعام 2001 للدول الأعضاء أن تمدّ نطاق التفتيش الذي كان محلّه جهاز كمبيوتر معيّن إلى غيره من الأجهزة المرتبطة به في حالة الاستعجال إذا كان يتواجد به معلومات يتمّ الدخول إليها في هذا الجهاز من خلال الجهاز محلّ التفتيش، فتنصّ المادة (19) من القسم الرابع على أنّه" من حق السلطة القائمة بالتفتيش الكمبيوتر المتواجد في دائرة اختصاصها أن تقوم في حالة الاستعجال بمدّ نطاق التفتيش إلى أيّ جهاز آخر إذا كانت المعلومات المخزّنة يتمّ الدخول إليها من الكمبيوتر الأصلي محلّ التفتيش" [2].

وعلى العكس من ذلك، هناك من التشريعات المقارنة ما تقصر أثر إذن التفتيش على الأجهزة الموجودة في مكان محدّد دون امتدادها إلى الأجهزة المرتبط مثل بلجيكا وسويسرا.

وتجدر الإشارة في هذا الصدد أنّه لمعرفة حكم تفتيش حاسوب مرتبط بالجهاز المأذون بتفتيشه والموجود داخل الدولة، نقوم بقياس هذه الحالة بالحالة التي يقوم صاحب المنزل المأذون بتفتيشه بإلقاء لفة أو حقيبة في أحد المنازل المجاورة. وحسمت محكمة النقض المصريّة [3] هذا الموقف حيث منعت المأذون بالتفتيش تعقب ما ألقي في المنزل المجاور، وذلك بدخوله وتفتيشه.

---

[1] قام المشرع الفرنسي بتعديل قانون الإجراءات الجنائية الفرنسي بموجب القانون رقم (239 لسنة 2003) بشأن الأمن الداخلي الصادر في 18 مارس سنة 2003، حيث أضاف المادة(57ـ1) من قانون الإجراءات الجناية والتي حسمت النزاع القائم حول مدى إمكانية تفتيش النظام الرئيسي و الأنظمة المتّصلة به في الداخل و الخارج.

- Article **17-1du LOI n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France** dispose que:" Les officiers de police judiciaire ou، sous leur responsabilité،les agents de police judiciaire peuvent، au cours d'une perquisition effectuée dans les conditions prévues par le présent code، accéder par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique، dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial.

[2] ينتقد بعض الفقهاء هذا النص مثل الدكتورة شيماء عبد الغني، حيث ترى بأنّ هذا النص يعطي للجهة القائمة بالتفتيش سلطة واسعة، خاصّة وأنّ كثيرا من أجهزة الكمبيوتر تتّصل بعضها ببعض في أنحاء العالم وبالتالي تمتد هذه السلطة إلى تفتيش أجهزة كثيرة و متعدّدة، بدون إذن لتلك الأجهزة، وهذا ما يتعارض مع ما تضمّنه ميثاق الحقوق والحريات الكندي في الفصل الثامن منه الذي ينص على حق الفرد في الحماية من التفتيش و الضبط غير المعقولين. انظر: د/ شيماء عبد الغني محمّد عطا الله، المرجع السابق، ص 300.

[3] نقض رقم 564, سنة 53 ق جلسة 13/ 06/ 1983, س 34.

إلاّ أنّ البعض يرى أنّ المجال هنا يفسح لإعمال حكم الفقرة الثانية من المادة (71) من قانون الإجراءات الجنائية المصري التي تنص على أنّ" للمندوب أن يجري أيّ عمل آخر من أعمال التحقيق أو أن يستجوب المتّهم في الأحوال التي يخشى فيها فوات الوقت متى كان متّصلا بالعمل المندوب له ولازما في كشف الحقيقة، إلاّ أنّ هذا الموقف غير صحيح، لأن تفتيش المنازل بغير رضا أصحابها محظور بنص الدستور– ولو في حالة الضرورة – إلاّ بناء على أمر قضائي مسبّب (المادة 44 من الدستور المصري). وفي مقابل ذلك يستطيع مأمور الضبط القضائي اتخاذ الإجراءات التحفظية اللازمة حتى يتم استصدار إذن التفتيش المطلوب من الجهة المختصة. ألا أننا نرى أنّ ذلك يتعارض مع خصائص الدليل الالكتروني، ذلك أنّه أثناء تحضير إذن تفتيش جديد بإمكان هذا الدليل أن يتبخر عمدا من قبل المتّهم ومن تمّ يخفي آثار جرمه، وهذا ما يؤدي إلى الإضرار بمصلحة العدالة.

وانطلاقا ممّا سبق ذكره نلاحظ أنّ ذاتية تفتيش الحاسوب وقصور القواعد التقليدية تظهر بصورة جليّة أثناء امتداد التفتيش إلى الأجهزة المرتبطة به من خلال الحالتين التاليتين:

1– إذا كانت الأجهزة المتّصلة بالجهاز الذي صدر إذن تفتيش بخصوصه ينتمي إلى شخص غير المتّهم، ومن تمّ يتعيّن تفتيش هذه الأجهزة المرتبطة به بناء على الإذن الأوّل وهذا ما يتناقض مع بعض التشريعات الإجرائية حيث تشترط صدور الأمر القضائي المسبب لتفتيش شخص غير المتهم في حالة ما إذا كانت النيابة العامة هي التي تتولّى التحقيق كالقانون المصري، وقد نصّ المشرّع على هذه الضمانة في الفقرة الثالثة من المادة (206) من قانون الإجراءات الجنائية المصري[1]. كما تثار شكوك في هذه الحالة إذا تمّ هذا التفتيش دون إخطار غير المتّهم أو من ينوب عنه[2].

2– الأصل أنّه في حالة التلبس لا يشترط الحصول مسبقا على إذن لتفتيش الجهاز حيث يمكن أن يرد التفتيش على الأجهزة المرتبطة، ومن تمّ يمكن التفتيش دون دخول مسكن غير المتّهم، فالانتقال غير مهمّ إلى مكان الجهاز الثاني بل إنّ ذلك يتمّ باستعمال وسائل تقنية حديثة "برامج الدخول"، فما مدى مشروعية استخدام تلك البرامج ؟ ألا يعدّ ذلك اعتداء على الحياة الخاصة للأفراد؟.

---

[1] تنص المادة (**206 فقرة الثالثة) على أنّه**: " ويشترط لاتخاذ أي إجراء من الإجراءات السابقة (تفتيش غير المتّهم أو منزل غير المتّهم) الحصول مقدّما على أمر مسبّب بذلك من القاضي الجزئي بعد اطلاعه على الأوراق"

[2] انظر المادة (83) من قانون الإجراءات الجزائيّة الجزائري.

الفرض الثاني: اتصال حاسب المتّهم بحاسب موجود في مكان آخر خارج الدولة:

من المشاكل التّي تواجه سلطات التحقيق في جمع الأدلة الالكترونية قيام مرتكبي الجرائم بتخزين بياناتهم في أنظمة تقنيّة خارج الدولة مستخدمين في ذلك شبكة الاتصالات البعدية وذلك بغرض عرقلة التحقيق ومن ثمّ سير العدالة. ونتيجة لذلك أدخلت تعديلات على قانون الإجراءات الجنائية لتجيز تفتيش الأنظمة المتّصلة حتّى ولو كانت متواجدة خارج إقليم الدولة، ومن ذلك القانون الفرنسي، حيث أجازت المادة(17 فقرة 2) من قانون الأمن الداخلي رقم (239 لسنة 2003) ، لمأمور الضبط القضائي أن يقوموا بتفتيش الأنظمة المتّصلة حتّى ولو تواجدت خارج الإقليم مع مراعاة الشروط المنصوص عليها في المعاهدات الدولية [1].

وفي نفس الاتجاه صدرت عن المجلس الأوربي توصيّات تجيز أن يمتدّ تفتيش الكمبيوتر إلى الشبكة المتّصل بها، ولو كانت تلك الشبكة تقع خارج إقليم الدولة. فتنص التوصية رقم (13 لسنة 1995) المتعلقة بالمشكلات القانونية لقانون الإجراءات الجنائية المتّصلة بتقنية المعلومات على أنّه " لسلطة التفتيش عند تنفيذ تفتيش المعلومات وفقا لضوابط معيّنة أن تقوم بمدّ مجال تفتيش كمبيوتر معيّن يدخل في دائرة اختصاصها إلى غير ذلك من الأجهزة مادامت مرتبطة بشبكة واحدة وأن تضبط البيانات المتواجدة فيها، مادام أنّه من الضروري التدخل الفوري للقيام بذلك".

كما نصّت التوصية رقم (17) على أنه "يمكن أن يمتدّ نطاق تفتيش الكمبيوتر إلى النظام المتواجد في الخارج، إذا كان من الضروري اتخاذ إجراءات عاجلة في هذا الشأن. ويتعيّن أن يوجد أساس قانوني لامتداد مجال هذا النوع من التفتيش، حتّى لا يشكل ذلك الإجراء مخالفة لسيادة دولة أجنبيّة لذلك فإنّه من الضروري الحصول على موافقة الدولة التي يمتدّ التفتيش إلى نظام يتواجد على إقليمها ".

وقد أجازت المادة (32) من الاتفاقية الأوربية بشأن جرائم الانترنت الموقعة عام2001، إمكانية الدخول بغرض التفتيش والضبط في أجهزة أو شبكات تابعة لدولة أخرى بدون إذنها في حالتين: الأولى إذا تعلّق التفتيش بمعلومات أو بيانات مباحة للجمهور، والثانيّة إذا رضي صاحب أو حائز هذه البيانات بهذا التفتيش.

---

[1] Article **17-1/2 du LOI n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France** dispose que: "S'il est préalablement avéré que ces données، accessibles à partir du système initial ou disponibles pour le système initial, sont stockées dans un autre système informatique situé en dehors du territoire national, elles sont recueillies par l'officier de police judiciaire, sous réserve des conditions d'accès prévues par les engagements internationaux en vigueur".

وعلى ذلك، إذا كان امتداد التفتيش إلى نظم الحاسوب الواقعة في إقليم بلد أجنبي(التفتيش الالكتروني العابر للحدود) له أهميته في إمكانية الحصول على الدليل عن بعد وفي بضع ثواني، إلاّ أنّ بعض الفقه يتحفظ على القيام بذلك لأنّه يعتبر انتهاك لسيادة الدولة الأجنبيّة، وإذا اقتضت ضرورة التحقيق القيام به ينبغي مراعاة العديد من الضمانات يكون متفق عليها سلفا عن طريق اتفاقيات و معاهدات في هذا المجال، وهذا ما يؤكد أهميّة التعاون الدولي في مكافحة الجرائم الالكترونيّة.

ولذلك تنتهي اللجنة الأوربية للمشكلات الجنائية التابعة للمجلس الأوربي في التوصية رقم (89) إلى القول بأنّ التفتيش و الضبط والإجراءات القسريّة الأخرى التي تقع على دولة أخرى تعتبر غير مشروعة إلاّ إذا كان القانون الدولي يجيزها .

2 ـ **شروط التفتيش في البيئة الالكترونية:**

تضمّنت معظم التشريعات الإجرائية على ضوابط معيّنة يجب إتباعها عند التعرّض للحريّات الشخصية بإجراء من الإجراءات الماسّة بالحريّة كالتفتيش و تنقسم الشروط العامّة للتفتيش إلى نوعين من الشروط، شروط موضوعيّة وأخرى شكليّة وذلك على النحو التالي:

أ ـ الشروط الموضوعية لتفتيش نظم الحاسوب: يقصد بهذه الشروط بصفة عامة الضوابط اللازمة لإجراء تفتيش صحيح، وهي في الغالب تكون سابقة له، ويمكن حصرها في ثلاث شروط أساسية هي: السبب، المحل، السلطة المختصة بالقيام به. وفيما يلي تفصيل كل شرط على حده:

1 ـ **سبب التفتيش في البيئة الالكترونية:** سبب التفتيش في الجرائم عموما هو السعي نحو الحصول على دليل في تحقيق قائم من أجل الوصول إلى حقيقة الحدث[1]، ويتمثل في وقوع جريمة ما جناية أو جنحة واتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها، وتوافر قرائن وأمارات قوية على وجود أشياء تفيد في كشف الحقيقة لدى المتّهم أو في مسكنه أو بشخص غيره أو مسكنه، وهو ما ينطبق على الجريمة الالكترونية على النحو التالي:

أوّلا: وقوع جريمة من الجرائم الالكترونية بالفعل سواء كانت جناية أو جنحة: لابدّ لصحّة إجراء التفتيش في بيئة تكنولوجيا المعلومات أن نكون بصدد جريمة الكترونية واقعة بالفعل سواء كانت جناية أو جنحة، وتستبعد المخالفات لضآلة خطورتها. وقد سبق بيان أنّه لا يوجد تعريف محدّد ومتّفق عليه بين الفقهاء حول مفهوم الجريمة الالكترونيّة وإن كنا انتهينا إلى تبنّي تعريف مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاقبة المجرمين المنعقد في فينا عام

---

[1] د/ قدري عبد الفتاح الشهاوي، المرجع السابق، ص 53.

2000، حيث عرّف الجريمة الالكترونية بأنها" **أيّة جريمة يمكن ارتكابها بواسطة نظام حاسوبي، أو شبكة حاسوبية، أو داخل نظام حاسوب ،وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الالكترونية** ".

وتطبيقا لمبدأ شرعيّة الجرائم والعقوبات، فلا محلّ لإصدار الإذن بتفتيش نظم الحاسوب إلا إذا كان المشرّع قد نصّ صراحة على الأفعال التي تشكل جرائم من هذا النوع، وذلك ما فعلته الكثير من التشريعات المقارنة، وفعله المشرع الجزائري من خلال القانون رقم (04ــ15) المؤرخ في 10 نوفمبر سنة 2004 حيث أدرج المشرع الجزائري فصلا خاصا ــ الفصل السابع ــ بجرائم المساس بأنظمة المعالجة الآلية للمعطيات. أمّا المشرع المصري لم يجرم جميع صور الإجرام الالكتروني، بخلاف المشرع الجزائري والفرنسي، بل اقتصر في الحماية على حماية برامج الحاسب الآلي و قواعد البيانات ضمن المصنّفات المشمولة بحماية حق المؤلف المنصوص عليها في المادة (181) من القانون رقم (82 لسنة 2002) والخاص بحماية حقوق الملكية الفكريّة[1]، بالإضافة إلى حماية البيانات الفرديّة الخاصة بالإحصاءات

---

[1] تعرض المشرع المصري لأول مرة لحماية برامج الحاسب الآلي من خلال القانون رقم(38 لسنة 1992), حيث تم تعديل نص المادة(20) من القانون رقم(354 لسنة 1953) الخاص بحماية حق المؤلف, بموجب المادة (2) من القانون رقم(38 لسنة 1992), وكان ذلك نتيجة مصادقة جمهورية مصر العربية على اتفاقية برن في 13ــ 7ــ 1976. وعند صدور قانون حماية حقوق الملكية الفكرية الجديد رقم(82 لسنة 2002) في 2 يونيه 2002, ونصّ في المادة الثانية منه على إلغاء القانون رقم (354 لسنة 1954). لمزيد من التفصيل حول تطور الحماية القانونية لمصنفات الحاسب الآلي انظر: د/ خالد مصطفى فهمي , الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون حماية الملكية الفكرية المصري, رقم 82 لسنة 2002 , دراسة مقارنة, دار الجامعة الجديدة, الإسكندرية, 2005, ص 36 و ما بعدها. وانظر كذلك: د/ محمود عبد الرحيم الديب , الحماية القانونية للملكية الفكرية, في مجال الحاسب الآلي و الانترنت, دار الجامعة الجديدة للنشر, 2005 , ص 28 و ما بعدها.

- أما المشرع الجزائري فقد أدرج برامج الحاسوب مثل نظيره المشرع المصري ضمن المصنفات الأدبية وذلك **بموجب الأمر رقم (03ــ** 05) و المتعلق بحقوق المؤلف والحقوق المجاورة حيث نصّت **المادة الرابعة** (4) منه على ما يلي:

" تعتبر على الخصوص كمصنفات أدبية أو فنية محميّة ما يأتي :

ــ المصنفات الأدبية المكتوبة مثل: المحاولات الأدبية, والبحوث العلمية و التقنية, و الروايات,والقصص, والقصائد الشعرية, **وبرامج الحاسوب**, والمصنفات الشفوية مثل المحاضرات والخطب, والمواعظ وباقي المصنفات التي تماثلها ".

وتجدر الإشارة إلى أنّ بعض الفقهاء ــ مثل الدكتور أمين مصطفى ــ يرى أنّ سياسة المشرّع المصري تميّزت بنوع من الخصوصيّة بشأن حماية حقوق الملكيّة الفكريّة, عن غيرها من الدول العربيّة, وذلك حينما خصّص المشرع المصري قانونا موحّدا لكافة حقوق الملكيّة الفكريّة سواء تعلّقت بحق المؤلف أوالملكيّة==

السكانيّة والبيانات الخاصة بالأحوال المدنيّة، وذلك في إطار القانون رقم (143 لسنة 1994). كما رصد حماية جنائية للتوقيع الالكتروني من خلال قانون تنظيم التوقيع الالكتروني رقم (15 لسنة 2004) من خلال المادة (23) من ذات القانون. أمّا باقي صور الإجرام الالكتروني لم يتعرّض لها ممّا أوجد فراغا تشريعيّا دفع الفقه إلى بسط سلطان قواعد قانون العقوبات التقليدية على هذه الجرائم وهو ما يتعارض مع مبدأ الشرعيّة ومبدأ حظر القياس في مواد التجريم والعقاب ممّا يتطلب تدخلاً تشريعيّا لسدّ هذا الفراغ التشريعي ومواجهة هذه الصور المستحدثة للإجرام الالكتروني.

ثانيا - اتهام شخص أو أشخاص معيّنين بارتكاب الجريمة أو المشاركة فيها: ينبغي أن تتوافر في حق الشخص المراد تفتيش شخصه أو مسكنه دلائل كافية تدعو للاعتقاد بأنه قد ساهم في ارتكاب الجريمة الالكترونيّة أو شريكا فيها ممّا يستوجب اتهامه فيها. ولم تتعرّض قوانين الإجراءات الجنائية لتعريف الدلائل، وإنّما اكتفت بالنص على تطلب الدلائل القوية والمتوافقة مع الاتهام[1]. إلاّ أنّ الفقه تصدّى لتحديد مفهومها حيث عرّفها بأنّها" مجموعة الوقائع الظاهرة والملموسة التي يستنتج منها أنّ شخصا معيّنا هو مرتكب الجريمة" [2].

أمّا الدلائل الكافية في الجرائم الالكترونيّة، يقصد بها "مجموعة المظاهر أو الأمارات المعيّنة القائمة على العقل والمنطق والخبرة الفنيّة والحرفيّة للقائم بالتفتيش والتي تؤيد نسبة الجريمة الالكترونية إلى شخص معيّن بوصفه فاعلا أو شريكا"[3]، ومن أمثلتها: ارتباط عنوان انترنت بروتوكول الخاص بجهاز الحاسوب الذي يحتوي على صور فاضحة مع رقم حساب المتّهم لدى مزوّد الخدمات، ووجود رقمين للتلفون لديه يستخدمان في ذلك[4].

ثالثا– توافر أمّرات قويّة أو قرئن على وجود بيانات أو معدّات معلوماتيّة تفيد في كشف الحقيقة لدى المتّهم المعلوماتي أو غيره: من المستقرّ عليه في التشريعات المقارنة أنّ الإذن

==الصناعية أو التجاريّة, بخلاف دول أخرى مثل تونس وعمان والكويت, حيث خصّص أكثر من قانون يتعلق بحقوق الملكية الفكرية. لمزيد من التفصيل انظر: د/ أمين مصطفى محمّد, الحماية الجنائيّة لحقوق الملكية الصناعية في ضوء الاتفاقيات الدولية والقوانين الوطنيّة, مجلّة الحقوق للبحوث القانونيّة والاقتصاديّة, جامعة الاسكندرية, العدد الثاني, 2007, ص 14 وما بعدها.

[1] انظر المواد(34، 350، 134) من قانون الإجراءات الجنائية المصري، والمواد(2ـــ 63، 105، 176, 177، 211، 212) من قانون الإجراءات الجنائية الفرنسي.

[2] د/ أحمد فتحي سرور، المرجع السابق، ص 755. وانظر أيضا في نفس المعنى:

Roger Merle et Andre Vitu, Traite de droit criminel, tome 2, quatrieme edition, Edition Cujas, Paris, 1989, P. 757.

[3] د/ هلالي عبد الله أحمد، المرجع السابق، ص 121.

[4] انظر: د/ شيماء عبد لغني، المرجع السابق، ص 282.

بالتفتيش يلزم أن يصدر بناء على تحريّت جدية، فلا يكفي لحث سلطة التحقيق إلى إصدار قرارها بالتفتيش مجرد وقوع جريمة من الجرائم الالكترونيّة، واتهام شخص معيّن بارتكابها، بل يجب أن تتوافر لدى المحقق أسباب كافية أنّه يوجد في مكان أو لدى الشخص المراد تفتيشه أدوات استخدمت في الجريمة الالكترونيّة، أو أشياء متحصّلة منها، أو أيّ أدلّة الكترونيّة يحتمل أن يكون لها فائدة في استجلاء الحقيقة لدى المتّهم أو غيره[1].

2: **محل التفتيش**:

يقصد بمحل التفتيش المستودع الذي يحتفظ فيه المرء بالأشياء الماديّة التي تتضمّن سرّه، و السّر الذي يحميه القانون هو ذلك الذي يستودع في محل له حرمة[2] كالمسكن أو الشخص و الرسائل. ومحل التفتيش في الجريمة الالكترونيّة هو الحاسوب و الشبكة التي تشمل في مكوّناتها الخادم والمزوّد الآلي والمضيّف و الملحقات التقنية .. .

ولكي يتمّ التفتيش على هذه المحال، فإنّه ينبغي الإشارة أنّ هذه الأخيرة لا تكون قائمة بذاتها، بل تكون إمّا موضوعة في مكان ما كالمسكن أو المكتب، أو تكون صحبة مالكها أو حائزها كما هو الشأن في الحاسوب المحمول أو هاتف نقال.

سبق وأن أشرنا إلى مدى قابليّة المكونات المادية والمعنوية للحاسوب فضلاً عن شبكات الاتصال الخاصّة به، وموقف التشريعات المقارنة من ذلك، فلا مجال لتكرار ذلك.

3: **السلطة المختصة بالتفتيش**:

ذكرنا سابقا أنّ التفتيش إجراء من إجراءات التحقيق الابتدائي التي تمسّ بالحرية الشخصية وانتهاك حرمة الحياة الخاصة للأفراد، لذلك حرص المشرّع الجنائي على إسنادها لجهة قضائية تكفل تلك الحريات والحقوق وتضمنها. إلاّ أنّ هذه التشريعات الجنائية لم تسر على نسق واحد فيما يخصّ تحديد الجهة التي يّعهد لها بالتحقيق الابتدائي لتكون صاحبة الاختصاص الأصيل بإجراء التفتيش، فقد ذهبت بعض القوانين كالتشريع المصري إلى منح هذه السلطة للنيابة العامة [3].

---

[1] USA v. Raymond Wong، App. 9th Cir، No. 02 -10070 CR-00-40069-CW،June 26، 2003.

[2] د/ قدري عبد الفتّاح الشهاوي، المرجع السابق، ص 110 و ما بعدها.

[3] كان المشرع المصري يأخذ بنظام الفصل ما بين سلطتي التحقيق والاتهام بموجب قانون تحقيق الجنايات الأهلي الصادر سنة1883. ثم عدل عن هذا القانون في(28 مايو1895)، حيث جمعت النيابة العامة في يدها سلطتي التحقيق والاتهام. ولما صدر قانون الإجراءات الجنائية بموجب القانون رقم150 لسنة1950 عاد مرة أخرى إلى نظام الجمع ما بين سلطتي التحقيق و الأتهام بيد النيابة العامة باستثناء جرائم معينة رأى أن يختص بها قاضي التحقيق وذلك بموجب المرسوم بقانون رقم(353 لسنة1952).

بخلاف الحال عند كل من الجزائر وفرنسا [1] حيث أخذت بنظام الفصل ما بين سلطتي الاتهام والتحقيق، حيث عهدت هذا الأخير لقاضي التحقيق، أمّا الأولى للنيابة العامة.

وإذا كان الأصل أنّ يقوم قاضي التحقيق أو النيابة العامة بإجراء التفتيش بنفسه ــ وهو نادر الحدوث عملا ــ ، إلاّ انّه يمكن لمأمور الضبط أن يقوم بذلك استثناء في حالتين[2]:

1 ــ التلبس و يجوز له تفتيش شخص المتهم في الجنايات و لجنح المعاقب عليها بالحبس مدة تزيد على ثلاثة أشهر(المادة 34، 46 إجراءات جنائية مصري).

2 ــ الانتداب من قبل المحقق المختص لتفتيش منزل أو شخص المتهم(المادة 70 إجراءات جنائية مصري)[3].

ولا يختلف الأمر في حالة الجرائم الالكترونيّة، فالأصل أن تقوم سلطة التحقيق الأصلية بتفتيش النظم المعلوماتية بنفسها أو ندب مأموري الضبط القضائي وفقا للقواعد الإجرائية المنصوص عليها في هذا الخصوص.

وفي هذه الحالة يجب أن يحدّد في إذن الندب بالتفتيش المكان المراد تفتيشه والشخص أو الأشياء المراد تفتيشها وضبطها (أجهزة الحاسوب ، صور جنسية الكترونيّة خاصة بالأطفال، مصنّفات الكترونية مقلّدة..)، والهدف من هذا التحديد في إذن التفتيش هو تجنب التفتيش الاستكشافي، بحيث لا يترك للمأذون بالتفتيش أي سلطة تقديرية في ذلك. إلاّ أنّ هناك صعوبة في احترام هذا الشرط أثناء الممارسة العمليّة في تفتيش أجهزة الكمبيوتر، ويرجع ذلك

---

[1] قام المشرع الفرنسي بتعديل قانون الإجراءات الجزائية بموجب القانون رقم(291ــ 2007) هادف إلــى تعزيــز قرينــة البــراءة و حقــوق المجنــي علــيهم **"la loi renforcant la protection de la presomption d'innocence et les droits des victimes"** ومن خلاله قــام باســتبدال مــصطلح **قاضي التحقيق** بهيئة أخرى سميت بـــ: **هيئة أو جماعة التحقيق** **"COllege D' instruction"** ويظهر ذلك من خلال نص **المادة (2) من القانون رقم(291ــ 2007)**، حيث جاء فيها:

"Dans les articles 80-1،80-1-1، 113-8، 116، 137-1، 137-2، 138،139،140، 141-1، 142، 144-1، 145،146، 147، 148، 148-1-1، 175، 175-1، 175-2، 176، 177، 179، 180، 181، 182، 184، 188، 197، 469، 495…du code du procédure pénale، les mots: "juge d'instruction" sont remplaces par les mots: "collège de l'instruction".

[2] انظر نقض 1937/11/1 مجموعة القواعد القانونية، جزء 4 ، ص 89 رقــم 105 و نقــض 17 / 6/ 1968 ، أحكام النقض السنة 19، ص 713، رقم 144 ونقض 20/ 12/ 1971 ، سنة 22، ص 801 ، رقم 192.

[3] وقد يعدّ هذا الندب في بعض الحالات مخالفة, كالحالة التي يفتّش **فيها مقر الصحفي** من قبل مأموري الضبط القضائي, لأنّ ذلك يعدّ مخافة لأحكام المادة (43) من القانون رقم 96 لسنة 1996 بشأن تنظيم الصحافة في مصر. لمزيد من التفصيل انظر: د/ أمين مصطفى محمّد, الحماية الجنائيّة الإجرائيّة للصحفي, دراسة في القانونين المصري والفرنسي, دار النهضة العربيّة, القاهرة, 2008, ص 56 وما بعدها.

إلى الطبيعة الخاصة لهذه الأخيرة الذي يحتوي بدوره على عدد كبير من الملفات، بالإضافة إلى أنّ أسماء هذه الملفات لا تدلّ بالضرورة على ما تحتويها، فقد يعمد المتهم إلى وضع أسماء مستعارة لملفات تحتوي على مواد غير مشروعة. كما تثار صعوبة قانونية أثناء تنفيذ إذن التفتيش على هذه الملفات، **فهل يعتبر كلّ ملف" صندوقا مغلقا " يحتاج كل واحد منها إلى إذن قضائي مستقل عن الآخر؟.**

ـ تضاربت أحكام القضاء الأمريكي فيما يخص هذه المشكلة، حيث اعتبرت من جهة أنّ الديسك بما فيه من ملفات وجهاز الكمبيوتر بما يحتويه من ملفات صندوقا مغلقا واحدا، ومن ثمّ لا يشترط صدور إذن قضائي مستقل لكل ملف على حده[1].

وعلى خلاف ذلك اتجهت أحكام أخرى للقضاء الأمريكي إلى أنّ كل ملف في الكمبيوتر يتطلّب إذنا خاصا لتفتيشه، وبناء على ذلك فإنّها اعتبرت أنّ الملف الواحد صندوق مغلق، ويرجع أساس هذا الحكم إلى اعتبار أنّ الكمبيوتر يحتوي على الكثير من المعلومات التي تتعلّق بالحياة الخاصة لصاحب هذا الجهاز، بمعنى اختلاط الملفات المجرمة مع البريئة، وإذا أجزنا لرجال الضبط القضائي فتح الملفات الأخرى الموجودة داخل الجهاز فإنّ ذلك سوف يؤدي بالفعل إلى الاعتداء على الحياة الخاصة للأفراد[2].

إلاّ أنّنا نعتقد أنّ مسلك القضاء الأمريكي في اضطراد أحكامه بخصوص مدى ضرورة صدور إذن تفتيش مستقل بخصوص تفتيش ملفات الحاسوب، له ما يبرره في الواقع العملي، فبإمكان الملف الواحد أن يحتوي على العديد من الملفات لاسيما مع التطور التقني الحديث للاتساع السّعة التخزينيّة لأجهزة الحاسوب، لذلك لا يعقل صدور أذون تفتيش بحسب عدد الملفات، هذا من جهة.

ومن جهة ثانية لا يتصوّر امتداد إذن التفتيش إلى كل ملفات الحاسوب لانّ إذن التفتيش ليس إذنا على بياض باستباحة حرمة الشخص أو حرمة مسكنه بغير قيد، ولكنّه مقيّد بالغرض منه، وهو ما تؤكده المادة (50 من قانون الإجراءات الجنائية المصري) على انّه لا يجوز التفتيش إلا للبحث عن الأشياء الخاصة بالجريمة الجاري جمع الاستدلالات بشأنها أو حصول التحقيق بشأنها. وانطلاقا من ذلك لا ينبغي تفتيش كل الملفات بإذن واحد لانّ الإذن الذي صدر في الأول خاص بجريمة محددة(مثلا جريمة قرصنة برامج) وبإمكان للمأذون أن يصادف أثناء تنفيذ الإذن جريمة عرضيّة أخرى مثل حيازة صور فاضحة للأطفال.

---

(1) USA v. Raymond Wong، 275 F .3d 449، 464-65 (5th Cir. 2001).

(2) USA v. Walser 275 F .3d 675، 986(10th Cir. 2001).

ب : الشروط الشكلية لتفتيش نظم الحاسوب:

بالإضافة إلى الشروط الموضوعيّة لصحة إجراء تفتيش نظم الحاسوب وشبكات الاتصال الخاصة به، هناك شروط أخرى ذات طابع شكلي يجب مراعاتها عند ممارسة هذا الإجراء صونا للحريّات الفرديّة من التعسّف أو الانحراف في استخدام السلطة، وتتمثل هذه الشروط في التالي:

1- الحضور الضروري لبعض الأشخاص أثناء إجراء التفتيش في البيئة الالكترونيّة: يعتبر هذا الشرط من أهم الشروط الشكليّة التّي يتطلّبها القانون في الجرائم التقليديّة، وذلك لضمان الاطمئنان إلى سلامة الإجراء وصحة الضبط.

بالنسبة لتفتيش الأشخاص لم تشترط التشريعات الإجرائية لصحته حضور شهود عند تفتيشهم، أما فيما يتعلق بتفتيش المساكن وما في حكمها، نجد أنّ المشرع المصري قد غاير في الشروط المقرّرة وفقا لشخص القائم به، حيث اشترط حضور شاهدين في حالة ما إذا كان التفتيش يباشر بمعرفة أحد مأموري الضبط القضائي، وعلى أن يكون هذان الشاهدان بقدر الإمكان من أقارب المتّهم البالغين أو من القاطنين معه بالمنزل أو من الجيران المادة (51) من قانون الإجراءات الجنائية المصري).

أما إذا كان القائم بالتفتيش هو قاضي التحقيق أو عضو النيابة العامة فيصحّ اتخاذ هذا الإجراء دون حاجة لاستدعاء شهود (المادة 92 إجراءات جنائية مصري)، ويستوي الأمر عند قيام مأمور الضبط القضائي بمباشرة التفتيش بناء على ذلك من سلطة التحقيق، فلا يلتزم باستدعاء شهود لأنّ المندوب يحلّ محلّ النائب تماما [1].

وعلى العكس من ذلك ينص القانون الجزائري والفرنسي على واجب حضور شاهدين في كلا الحالتين سواء كان القائم بالتفتيش قاضي التحقيق أو ضابط الشرطة القضائية، ويعدّ حضور شاهدين إحدى الأشخاص الواجبة الحضور وقت إجراء تفتيش مسكن المتهم، لأنّه يشترط أوّلاً حصول التفتيش بحضور المتّهم، فإذا تعذّر عليه الحضور وقت ذلك الإجراء، كان على ضابط الشرطة القضائية أن يكلّفه بتعيين ممثل له، وإذا امتنع أو كان هاربا، استدعى ضابط الشرطة القضائية لحضور تلك العمليّة شاهدين من غير الموظفين الخاضعين لسلطته[2].

---

[1] د/ هلالي عبد الله أحمد، المرجع السابق، 165.

[2] انظر المادة (45) من قانون الإجراءات الجزائية الجزائري، والتي هي ترجمة حرفية للمادة (56) إجراءات جنائية فرنسي.

ويلاحظ أنّ التعديل الذّي أدخله المشرع الجزائري على قانون الإجراءات الجزائية بموجب القانون رقم (06ـ 22) مسّ المادة (45) منه حيث استغنى المشرع عن ضمانة حضور الأشخاص المحدّدين في الفقرة الأولى من هذه المادة في جرائم معيّنة منها جرائم المساس بأنظمة المعالجة الآلية للمعطيات. والحكمة من ذلك ترجع إلى ضرورة إضفاء نوع من السريّة أثناء جمع الدليل الالكتروني، خاصة وأنّ هذا الدليل ذو طبيعة خاصة من حيث سرعة تعديله و التلاعب فيه حتى عن بعد. كما أنّ هذه الضمانة بدأت تتضاءل أهميّتها في الدول التي بدأت تأخذ بإجراء "التفتيش عن بعد"[1]، أو ما يطلق عليها في الفقه الفرنسي مصطلح "التفتيش على المباشر" (Perquisition en ligne)[2] .

2 ـ **الميقات الزمني لإجراء التفتيش في الجرائم الالكترونيّة:** يقصد بضمانة الميقات في التفتيش أن يجريه القائم به خلال فترة زمنيّة عادة ما يحدّدها المشرّع، وذلك حرصا على تضييق نطاق الاعتداء على الحريّة الفردية وحرمة المسكن، في حين نجد بعض التشريعات الإجرائية تركت أمر تحديد ذلك الوقت للقائم بالتفتيش ومن تمّ يقوم به في كل الأوقات سواء ليلا أو نهارا، ومن بين تلك التشريعات قانون الإجراءات الجنائية المصري.

وعلى العكس من ذلك نجد القانونين الجزائري والفرنسي يحظران تفتيش المنازل وما في حكمها في وقت معيّن، وهو محدّد في القانون الجزائري من الساعة الخامسة صباحا إلى الساعة الثامنة مساء، وذلك من خلال المادة 47اجراءات جزائية[3]، أما في القانون الفرنسي فنجده محدّدا من الساعة السادسة صباحا إلى الساعة التاسعة مساء، وذلك من خلال المادة (59) إجراءات جنائية[4].

إلاّ أنّ هناك حالات استثنائية يصح فيها إجراء التفتيش ليلا أو نهارا، تتمثل فيما يلي:

---

[1] يقصد بالتفتيش عن بعد: قيام مأمور الضبط القضائي بالتفتيش وهو قاعد في مكتبه باستخدام برامج خاصة تحمل في طابعها قاعدة التفتيش عن الجريمة، ويثير هذا الإجراء العديد من المشكلات القانونية، أبرزها:
ــ التعدي على الخصوصيّة. ــ التعدّي على سيادة دول أخرى، ذلك لأنه يعدّ من قبيل التجسس وانتهاك حواسيب وخوادم لهذه الدول، خاصة إذا كانت من الدول التي لا تعترف بمشروعيّة هذه البرمجيات.

[2] Yann Padova, un aperçu de lutte contre la cybercriminalité en France, revue de science criminelle et de droit pénale, n^0 4, Dalloz,2002, p. 770.

[3] تنص المادة (47) إجراءات جزائية جزائري على" لا يجوز البدء في تفتيش المساكن أو معاينتها قبل الساعة الخامسة صباحا، ولا بعد الساعة الثامنة مساء، إلاّ إذا طلب صاحب المنزل أو وجهت نداءات من الداخل أو في الأحوال الاستثنائية المقرّرة قانونا".

([4]) Article 59 alinéa 1 du C.P.P.F، dispose que :" Sauf réclamation faite de l'intérieur de la maison ou exceptions prévues par la loi, **les perquisitions et les visites domiciliaires ne peuvent être commencées avant 21 6 heures et après 21 heures.**

- حالة رضا صاحب المنزل رضا حرا، صريحا وعن علم بالسبب.
- حالة الضرورة وتتمثّل في حالة الاستغاثة من داخل المنزل، وحالتي الحريق والغرق[1] أو ما شابه ذلك.
- التحقيق في جميع الجرائم المعاقب عليها في المواد(342 إلى 348) من قانون العقوبات الجزائري وذلك في داخل كل فندق أو منزل مفروش أو فندق عائلي أو محل لبيع المشروبات أو نادي أو منتدى أو مرقص أو أماكن المشاهدة العامة وملحقاتها، وفي أي مكان مفتوح للعموم أو يرتاده الجمهور، إذا تحقّق أنّ أشخاصا يستقبلون فيه عادة لممارسة الدعارة.
- في الأحوال الاستثنائية المقرّرة قانونا كأوقات الطوارئ طبقا لنص المادة (11) في قانون(1955/4/3) وكذا ما تنص عليه المادة 77 من حق مفتّش الصحّة والبوليس في دخول المستشفيات[2].
- بالإضافة إلى جريمتي المخدرات والإرهاب التي أجاز فيهما المشرع الجزائري مأمور الضبط القضائي إجراء التفتيش في كل ساعة من ساعات النهار أو الليل، أضاف قائمة من الجرائم وذلك من خلال المادة (10) من القانون رقم (06ـــ 22) المعدّل والمتمّم للأمر رقم (66ـــ 155) والمتضمن قانون الإجراءات الجنائيّة، وتتمثل هذه الجرائم في: الجريمة المنظّمة عبر الحدود الوطنية، **الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات** وجرائم تبييض الأموال وكذا الجرائم المتعلّقة بالتشريع الخاص بالصرف[3].

---

[1] تجدر الإشارة أنّه في هذه الحالات إذا كان يجوز فيها لمأمور الضبط القضائي الدخول الليلي في المسكن، إلاّ أنّه لا يجوز تفتيشه، بل له الحق فقط في إلقاء النظر على محتوياته دون معاينتها وفحصها، ولما كان دخول المسكن عملا مشروعا، وكانت حالة التلبس قائمة فيه، فله أن يباشر سلطاته المقرّرة في القانون، وهي القبض على المتّهمين وتفتيشهم وضبط كل ما يفيد في كشف الحقيقة. انظر: د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، ، الطبعة الثانية، دار النهضة العربة، القاهرة، 1988، ص 580. وانظر أيضا: د/ عوض محمد عوض، التفتيش في ضوء أحكام النقض، دراسة مقارنة، بدون دار النشر، الإسكندرية، 2006، ص 87.

[2] د/ إبراهيم محمد إبراهيم محمّد، النظريّة العامة لتفتيش المساكن في قانون الإجراءات الجنائيّة، دراسة مقارنة، رسالة دكتورا، كليّة الحقوق، جامعة القاهرة، 2005، 337. وانظر أيضا: د/ سامي حسين الحسيني، المرجع السابق، ص 296.

[3] تنص المادة (3/47) المعدلة بالمادة (10) من القانون رقم(06ـــ 22) المعدّل والمتمّم للأمر رقم (66ـــ 155) والمتضمن قانون الإجراءات الجنائيّة ما يلي:" وعندما يتعلّق الأمر بجرائم المخدرات أو الجريمة المنظّمة عبر الحدود الوطنية، **الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات** وجرائم تبييض الأموال و الإرهاب وكذا الجرائم المتعلّقة بالتشريع الخاص بالصرف فإنّه يجوز إجراء التفتيش و المعاينة والحجز في كل محل سكني أو غير سكني **في كل ساعة من ساعات النهار أو الليل** وذلك بناء على إذن مسبق من وكيل الجمهوريّة المختص".

ويلاحظ أنّ المشرّع الجزائري عندما استثنى الجرائم الماسّة بأنظمة المعالجة الآلية للمعطيات من حظر التفتيش ليلا، يكون قد أدرك فعلا ميزة هذه الجرائم، من حيث قابلية الدليل الالكتروني فيها للمحو والتدمير في أقل من ثانية، لذلك أنّ إرجاء التفتيش في الموعد القانوني قد يعرقل السير الطبيعي لمجريات التحقيق.

أمّا بالنسبة للتشريعات التي لم تنصّ صراحة على مواعيد خاصة لإجراء التفتيش في الجرائم الالكترونيّة، فتسري عليها القواعد العامة التي تحدّد الميقات الزمني لإجراء التفتيش في الجرائم التقليديّة.

3 ـ **محضر التفتيش في الجرائم الالكترونية:** باعتبار أنّ التفتيش عمل من أعمال التحقيق، فينبغي تحرير محضر يثبت فيه ما تمّ من إجراءات، وما أسفر عنه التفتيش من أدلة، ولم يتطلّب القانون شكلا خاصا في محضر التفتيش، وبالتالي فإنّه لا يشترط لصحّته سوى ما تستوجبه القواعد العامة في المحاضر عموما، والتي تقتضي بأن يكون مكتوبا باللغة الرسميّة وأن يحمل تاريخ تحريره وتوقيع محرره وأن يتضمّن كافة الإجراءات التي اتخذت بشأن الوقائع التي يثبتها.

ونفس الأمر بالنسبة لمحضر تفتيش نظم الحاسوب، فإنّه يستلزم بالإضافة إلى الشكليّات السابقة ضرورة إحاطة قاضي التحقيق أو عضو النيابة بتقنيّة المعلومات، ثمّ ينبغي بعد ذلك أن يكون هناك شخص متخصّص في الحاسوب والانترنت يرافقه للاستعانة به في مجال الخبرة الفنيّة الضروريّة، وفي صياغة مسودّة محضر التفتيش.

هذا فيما يخص بالتفتيش كأهم إجراء من إجراءات جمع الأدلة في مجال البيئة الالكترونية، وسنتناول فيما يلي الضبط كإجراء مستقل عن التفتيش على الرغم من أنّ التشريعات الإجرائية عادة ما تجمع بينهما باعتبار أنّ ضبط الأشياء المتعلقة بالجريمة هي الأثر المباشر للتفتيش، إلاّ انّه من الممكن أن يكون الضبط نتيجة لمعاينة، كما يجوز للمحقق أن يطالب أحد الأفراد بتقديم شيء موجود في حيازته إليه و يلزمه بذلك، و يطلق على الإجراء " الالتزام بالعرض"[1].

---

[1] وفي ذلك تنص المادة (99) من قانون الإجراءات الجنائية المصري على أنّ " لقاضي التحقيق أن يأمر الحائز لشيء يرى ضبطه أو الاطلاع عليه بتقديمه .."

ثالثا: الضبط

يختلف الضبط[1] في الجريمة الالكترونية عن الضبط في غير ذلك من الجرائم من حيث المحل، وذلك بسبب أنّ الأوّل يرد على أشياء ذات طبيعة معنويّة وهي البيانات، المراسلات والاتصالات الالكترونية، أمّا الثاني فيرد على أشياء ماديّة، منقولة كانت أم عقارات، و قد أثارت هذه الطبيعة المعنوية للبيانات جدلا فقهيّا واختلافا تشريعيّا حول مدى إمكانية ضبطها خاصة إذا كانت مجردة من الدعامة المادية المثبّتة عليها، ويرجع السبب في ذلك أنّ الضبط ــ حسب الأصل ــ لا يرد إلاّ على الأشياء المادية [2].

وإذا كان الأمر قد انتهى بنا إلى ضرورة أن يشمل التفتيش المكوّنات المعنوية للحاسوب، فانّه من الضروري أن يترتّب على ذلك إباحة ضبطها، وان كان هذا الأمر قد يواجه صعوبات كثيرة من الناحية التشريعيّة لعدم وجود نصوص خاصة بذلك، خاصة التشريعات العربية ومنها التشريعان الجزائري والمصري، وذلك بخلاف التشريع الفرنسي حيث تمّ إدخال تعديلات على قانون الإجراءات الفرنسي لسدّ هذا الفراغ التشريعي وذلك بموجب قانون الأمن الداخلي رقم 239 لسنة 2003 حيث استحدث المادة (76ــ 1 فقرة 3) التي تنص على أنّ البيانات التي يتم الحصول عليها من جراء تفتيش النظام المعلوماتي يتعين نسخها على دعامات، ثمّ يتم تحريز هذه الدعامات في أحراز مختومة بالشمع الأحمر [3]، وهذا الأمر شيء طبيعي كون فرنسا من الدول الموقعة على اتفاقية بودابست لعام 2001، ونصت هذه الأخيرة على الضبط في المادة (19) من القسم الرابع منها على أنّه" من سلطة كل دولة طرف أن تتخذ الإجراءات التالية: ــ أن تضبط نظام الكمبيوتر أو جزءا منه أو المعلومات المخزنة على أي وسيط من وسائط التخزين الخاصة بالكمبيوتر، وأن تحافظ على سلامة تلك المعلومات المخزنة ".

---

[1] يقصد بالضبط في قانون الإجراءات الجنائية: "وضع اليد على شيء يتصل بجريمة وقعت و يفيد في كشف الحقيقة عنها و عن مرتكبها ". انظر: د/ مأمون سلامة، المرجع السابق، ص 358.

[2] لمزيد من التفصيل حول هذه الاختلافات انظر: د/ هشام محمد فريد رستم ، المرجع لسابق، ص 93 و ما بعدها. وانظر أيضا: د/ هلالي عبد الله أحمد، المرجع السابق، ص 199 و ما بعدها. أيضا د/ عبد الفتاح بيومي حجازي، المرجع السابق، 218 و ما بعدها.

[3] Article **17-1/3 du LOI n° 2003-239 du 18 mars 2003 pour la sécurité intérieure en France** dispose que:" - « Les données auxquelles il aura été permis d'accéder dans les conditions prévues par le présent article peuvent être copiées sur tout support. Les supports de stockage informatique peuvent être saisis et placés sous scellés dans les conditions prévues par le présent code. ».

وتجدر الإشارة إلى أنّ الضبط قد يرد على عناصر معلوماتية منفصلة مثل الديسكات والاسطوانات الممغنطة.. ، وهنا لا تثور أيّ مشكلة قانونية عند القيام بالضبط، ولكن الصعوبة تثار عندما يلزم ضبط **النظام كله أو الشبكة كلها**، ذلك لأنّها تحتوي على عناصر لا يمكن فصلها، ومع ذلك يتعيّن ضبطها لأنّها تتضمّن عناصر للإثبات في الجريمة ، لذلك يتّم **إعمال مبدأ التناسب** [1] من أجل إقامة التوازن بين مصلحتين، مصلحة الدولة في كشف الحقيقة ومصلحة صاحب النظام في تسيير أعماله وعدم ضياع فرص الربح خاصة في المشروعات الاقتصادية، وقد قضت المحكمة الفدرالية الألمانية بإلغاء قرار الضبط الذي ورد على 220 دسك بالإضافة إلى الوحدة المركزية وذلك اثر مخالفة مبدأ التناسب [2].

وأمّا بالنسبة للمكونات المادية للحاسوب فلا يثير ضبطها أيّ مشكلات، فيمكن ضبط الوحدات المعلوماتية الآتية: وحدة المدخلات بما تشمله من مفردات كلوحة المفاتيح، نظام الفأرة، نظام القلم الضوئي...، وضبط وحدة المخرجات وما تشمل عليه من وسائل كالشاشة، الطابعة، الرسم والمصغرات الفيلمية.. ، أيضا وحدات التخزين كالأقراص الصلبة والمرنة وأقراص الليزر.

ومن الطبيعي أن تختلف طريقة ضبط البيانات المعالجة آليّا عمّا هو متّبع عند ضبط الأشياء المحسوسة كجهاز الحاسب الآلي وملحقاته كالأقراص المرنة والمودم والخادم ..[3]، فهناك أسلوب **النسخ (Copy)** وحاليا يتمّ استخدام برامج متخصصة في النسخ مثل برنامج (Lap Link) ، كما يوجد أسلوب **تجميد التعامل بالحاسوب** أو إحدى القطع المكوّنة له التي استخدمت في ارتكاب الجريمة، ويتّخذ هذا الأسلوب عدّة مظاهر، من أبرزها: نظام ضغط محتويات القرص الصلب، وكذلك نقل تلك المحتويات إلى أقراص صلبة متعددة أو ممغنطة. ومثل هذا الإجراء يصلح أن يتخذ في مواجهة الحاسبات الخادمة التي تحتوي على مواقع

---

(1) يقصد بهذا المبدأ (Principe de proportionnalité): " اقتصار الضبط على الأدلة التي تفيد في كشف الحقيقة، بحيث لا يؤدي الضبط إلى تعطيل كل العمل في النظام و الشبكات المتصل بها". انظر د/ شيماء عبد الغني محمد عطا الله، المرجع السابق، ص 358.

(2) Verguchi Pascal, la répression de délit informatique dans une perspective international, thèse, Montpellier, 1996, p. 365.

مشار إليه عند: د/ انظر د/ شيماء عبد الغني محمد عطا الله، المرجع السابق، نفس الموضع.

(3) ونتيجة لذلك يفضل البعض فضلا عن المصطلح التقليدي " الضبط"(**Saisir**) استخدام مصطلح " **الحصول بطريقة مشابهة**"(**Obtenir par un moyen similaire**) وذلك من أجل الأخذ في الاعتبار الطرق الأخرى لرفع البيانات غير المادية، وهو ما نستشفه في(الفقرة 3 من المادة 19) من الاتفاقية الأوربية لجرائم الانترنت.

الدعارة ، مواقع الهكرة أو ملفات فيروسية، كما يصلح أيضا إذا كان القرص الصلب يحتوي مثلا على ملفات مشفرة، و تحتاج إلى فكّ شفرتها [1].

والمعروف أنّ بعد ما يتمّ ضبط البيانات الالكترونية يتعيّن تحريزها و تأمينها فنيّا[2] خاصة أمام غياب الثقافة المعلوماتية عن المحقق الجنائي ممّا يجعل تلك الأدلة عرضة للإتلاف والإفساد، لذلك يتعيّن اتخاذ بعض الإجراءات الخاصة للحفاظ عليها وصيانتها من العبث، وذلك على النحو التالي[3] :

1ــ ضبط الدعائم الأصلية للبيانات وعدم الاقتصار على ضبط نسخها.

2ــ عدم تعريض الأقراص والأشرطة الممغنطة لدرجات الحرارة العالية ولا إلى الرطوبة، مع الإشارة إلى أنّ درجة الحرارة المسموح بها تتراوح مابين (2 ــ 32) درجة مئوية، أما بالنسبة للرطوبة المسموح بها فتتراوح ما بين (20% إلى 80%).

3ــ منع الوصول إلى البيانات التي تمّ ضبطها أو رفعها من النظام المعلوماتي: نص على هذا الإجراء المادة (19 فقرة الثالثة) من اتفاقية بودابست الموقعة في 23 نوفمبر 2001، ويتمّ اللّجوء إلى هذا الإجراء في حالة ما إذا كانت البيانات تتضمن خطرا أو ضررا بالمجتمع ومثال ذلك: البرامج التي تحتوي على فيروسات أو تقدّم نموذجا لعمل فيروسات، أو قنابل أو في الحالات التي تكون فيها محتوى البيانات غير مشروع كما في حالة المواد الإباحية الطفولية. ولا يقصد بهذه العبارة "الرفع" (enlèvement) تدمير البيانات بل تستمر في الوجود، إلاّ أنّه يتمّ حرمان المشتبه فيه من الولوج إليها، لكن يمكن إعادتها إليه بعد التحقيق الجنائي. ومن التشريعات التي أخذت بهذا الإجراء قانون تحقيق الجنايات البلجيكي، وذلك من خلال المادة (29 مكرر/ 3) حيث أعطى للنيابة العامة سلطة الأمر بغلق هذه البيانات (Blocage de données) لمنع الوصول إليها، أو إلى النسخة المستخرجة منها الموجودة لدى من يستعملون النظام[4].

---

[1] د/ عمر أبوبكر بن يونس، المرجع السابق، ص 871 وما بعدها .

[2] فضلا عن هذه القواعد التأمينية، يتعيّن اتخاذ الإجراءات التّي وضعها المشرع للمحافظة على سلامة المنقولات عامة، راجع وفي ذلك المواد التالية: (55، 56، 98، 199، 157) إجراءات جنائية مصري، و المواد (45 و 84) إجراءات جزائية جزائري.

[3] د/ هشام محمد فريد رستم، المرجع السابق، ص129 وما بعدها.

[4] Meunier (C), la loi du 28 novembre, 2000, relative a la criminalité informatique, revue . dr. Pen.et de Crim. 2002. P. 674.

الفرع الثاني
الإجراءات الشخصيّة

سنتطرق في التالي لمجموعة أخرى من الإجراءات التقليدية ذات الطبيعة الشخصيّة لأنّه غالبا ما يتوسّط فيها الشخص بين القيام بالإجراء والحصول على الدليل وتتمثّل هذه الإجراءات في: **التسرب، الشهادة والخبرة التقنيّة**، واذا كان بعضها مستحدثا من قبل المشرع الجزائري كعملية التسرب مثلا، إلاّ أنّ مضمونها ذات طابع تقليدي، أمّا بالنسبة للشهادة سنتعرف من خلالها على أشخاص ذي طبيعة خاصة من الشهود في مجال الجريمة الالكترونية، ومدى إلزامهم بإدلاء بعض البيانات المعلوماتيّة ذات نوع من الخصوصية، وبعد ذلك نتطرق الخبرة باعتبارها الملجأ الأمين للمحقق و القاضي في مثل هذه النوعيّة من الجرائم وذلك كنهج يستقى منه الدليل الرقمي ، بما يمكن معه القول إنّ الخبرة في الجرائم الالكترونية قد تكون هي الحل الحاسم لاسيما في الدول التي لا تزال تعاني من تخلف ربط تكنولوجيا المعلومات بالهيكلة القضائيّة فيها، وهو قول صحيح نسبيا، إلا أنّ القصور سوف يبدو واضحا إذا تأملنا دور الخبرة وقدرتها على مواصلة النهج بما يجعلها قابلة للخضوع لمبدأ حريّة القاضي في تكوين عقيدته، بحيث يجب ألاّ تتجاوز هذا المبدأ إلى ما يجعل القاضي يخضع لما تنتهي إليه من نتائج، فمثل هذا الأمر يجعل من الخبير قاضيا دون شك.

أوّلا: عمليّة التسرب

استحدث المشرع الجزائري في مجال مكافحته جرائم المساس بأنظمة الحاسب الآلي عدّة إجراءات للكشف عن الجريمة ومرتكبيها وتقديمهم للعدالة لينالوا جزاء عما اقترفوه من جرم في حق المجتمع، وترجع العلّة في استحداث مثل هذه الإجراءات إلى عجز أساليب البحث والتحري التقليديّة والتي لم تعد كافيّة وفعالّة للكشف عن الجرائم المستحدثة من بينها الجريمة الالكترونيّة، وتتمثل هذه الإجراءات في عمليتين:الأولى هي **عملية التسرب**، **أمّا الثانيّة فهي:اعتراض المراسلات وتسجيل الأصوات والتقاط الصور**. وسنتناول فيما يلي إجراء التسرب فقط، ذلك أنّ الثاني دو طبيعة معلوماتية، حيث تستعمل فيه الوسائل التقنيّة في التحري والتحقيق، لذلك ندرجه ضمن الإجراءات الحديثة لجمع الدليل الالكتروني.

أدرج المشرع الجزائري عمليّة التسرب بموجب القانون رقم (06ـــ 22) المؤرخ في (20 ديسمبر 2006)، الموافق لـــ 29 ذي القعدة لسنة 1427هجريّة، المعدّل والمتمّم للأمر رقم (66ـــ 155) المتضمن قانون الإجراءات الجزائيّة، والذي أفرد الفصل الخامس منه تحت عنوان: "**في التسرب**" والذي تضمّن ثمانية مواد(من المواد 65مكرر11 حتّى المادة 65

مكرر18). وتناول من خلالها تحديد مفهوم هذه العملية، وشروط إجراءها، العمليات المبررة، وأخيرا الحمايّة الجنائية للقائم بعمليّة التسرب. وسنحاول تفصيل ذلك من خلال النقاط التاليّة:

1- مفهوم عملية التسرب: عرّف المشرّع التسرّب في المادة (65 مكرر 12)، وان كان في الأصل أنّ التعريفات من عمل الفقه، ويرجع سبب ذلك إلى حداثة وخطورة هذا الإجراء.

ويقصد بالتسرب: قيام ضابط أو عون الشرطة القضائية تحت مسؤولية ضابط الشرطة القضائية المكلّف بتنسيق العمليّة بمراقبة الأشخاص المشتبه في ارتكابهم جناية أو جنحة بإيهامهم أنّه فاعل معهم أو شريك أو خاف. ويلجأ إلى هذا الإجراء عادة عندما تقتضي عمليّة التحري أو التحقيق في إحدى الجرائم المذكورة في المادة (65 مكرر) من هذا القانون وهي: - جرائم المخدرات - الجريمة المنظمة عبر الحدود الوطنيّة - الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات - جرائم تبييض الأموال والإرهاب - وأيضا الجرائم المتعلّقة بالتشريع الخاص بالصرف.

ويمكن تجسيد عملية التسرب في الجرائم الالكترونية كاشتراك ضابط أو عون الشرطة القضائية في محادثات غرف الدردشة أو حلقات النقاش حول دعارة الأطفال أو كلام يدور حول قيام أحدهم باختراق شبكات أو بث فيروسات، فيتّخذ المتسرب أسماء مستعارة ويظهر بمظهر طبيعي كما لو كان فاعل ممثلهم ويحاول الاستفادة من معرفتهم حول كيفية اقتحام الهاكر لموقع ما، أو مباشرة الحديث في الموضوع الجنسي حتّى يتمكنوا من اكتشاف وضبط الجرائم التي تتمّ من خلالها كالدعوة للدعارة مثلا.

2- **شروط صحّة عمليّة التسرب:** التسرب كممارسة غير عادية للضابط أو عون الشرطة القضائيّة ، بل يعدّ من أخطر الإجراءات مساسا بحرمة الحياة الخاصة للمتّهم، لذلك اشترط المشرع ضمانات معيّنة يتعيّن مراعاتها عند اللجوء إلى هذا الإجراء ويتمثل ذلك فيما يلي:

أ - صدور إذن التسرب من وكيل الجمهوريّة أو قاضي التحقيق بعد إخطار وكيل الجمهوريّة.

ب - يجب أن يكون الإذن مكتوبا مع احتوائه على الأسباب التي تبرر صدوره، أي وجوب أن يكون مسببا.

ج - يذكر في الإذن الجريمة التي تبرر اللجوء إلى هذا الإجراء، وهويّة ضابط الشرطة القضائيّة الذي تتمّ العمليّة تحت مسؤوليته.

ج - يحدّد في الإذن مدّة عمليّة التسرب التي لا يمكن أن تتجاوز أربعة (4) أشهر، ويمكن أن تجدّد حسب مقتضيات التحرّي أو التحقيق، ضمن نفس الشروط الشكليّة والزمنيّة، وفي نفس

الوقت اجاز القانون للقاضي الذي رخص بإجرائها أن يأمر في أيّ وقت بوقفها قبل انقضاء المدّة المحدّدة .

وانطلاقا مما سبق ذكره نلاحظ أن المشرع الجزائري أسند مهمة إصدار إذن التسرب إلى وكيل الجمهورية أو قاضي التحقيق بعد إخطار وكيل الجمهوريّة، بمعنى أن المشرع خرج عن الأصل العام في التحقيق القائم على الفصل بين سلطتي الاتهام والتحقيق، ذلك أن وكيل الجمهورية مهمته الأساسيّة هي تقديم المتهم إلى العدالة، ومن الصعوبة أن يتجرد من صفته الاتهاميّة عندما يقوم بإصدار الترخيص بالتسرب، خاصة وأن طبيعة عمليّة التسرب فيها نوع من الخطورة على حرمة الحياة الخاصة للأفراد لاسيما الحق في الخصوصيّة، لذلك فالأفضل منح هذه المهمة إلى قاضي التحقيق لما له من استقلالية وحسن التقدير ما يطمئن معه الأفراد. هذا من جهة.

ومن جهة أخرى، بالرغم من أهميّة هذا الإجراء في الكشف عن الفكرة الإجرامية والتي قد لا تظهر للوجود دون اللجوء إلى عملية التسرب، إلاّ أنه يطرح انتقادات كالتي يطرحها التحريض البوليسي، حيث يلعب المتسرب دورا ايجابيّا أثناء القيام بالأعمال الإجرامية، وذلك شيء ضروري حتى يكتسب ثقة المشتبه فيهم، خاصة وأنّ طبيعة هذا الأخير دو نسبة عالية من الذكاء . **إذن فما مدى مسؤولية المتسرب عن الأفعال التي يرتكبها ؟** وقبل الإجابة على هذا السؤال ينبغي علينا بيان الأفعال التي أباحها المشرّع للضابط أو العون المتسرب .

3 ـ الأفعال المبرّرة في عمليّة التسرب: نص المشرع صراحة في المادة (65 مكرر 14) على أنّه يمكن لضباط وأعوان الشرطة القضائيّة المرخص لهم بإجراء عمليّة التسرّب والأشخاص الذين يسخّرون لهذا الغرض القيام بما يلي[1]:

---

[1] تجدر الإشارة أن صياغة هذه الأفعال مأخوذة من المادة(706ـ 32) من قانون الإجراءات الجنائية الفرنسي، وذلك في إطار مكافحته جريمة الاتجار غير مشروع للمخدرات .

Article 706-32 du CCP francais dispose que " ...les agents de police judiciaire peuvent، avec l'autorisation du procureur de la République ou du juge d'instruction saisi des faits qui en avise préalablement le parquet, et sans être pénalement responsables de ces actes :

1- Acquérir des produits stupéfiants ;

2- En vue de l'acquisition de produits stupéfiants، mettre à la disposition des personnes se livrant à ces infractions des moyens de caractère juridique ou financier ainsi que des moyens de transport, de dépôt, d'hébergement، de conservation et de télécommunication. "

- اقتناء أوحيازة أو نقل أو تسليم أو إعطاء مواد أو أموال أو منتوجات أو وثائق أو معلومات متحصّل عليها من ارتكاب الجرائم أو مستعملة في ارتكابها.
- استعمال أو وضع تحت تصرف مرتكبي هذه الجرائم الوسائل ذات الطابع القانوني أو المالي وكذا وسائل النقل أو التخزين أو الإيواء أو الحفظ أو الاتصال.

ومن خلال هذا النص يتضح لنا أن طبيعة هذه الأفعال تستوجب من القائمين بها مشاركة إيجابيّة، كحيازة متحصلات الجريمة أو وسائل ارتكابها، وهذا النوع من الأفعال له تأثير على المسؤوليّة الجزائيّة، إلاّ أن القانون أعفاهم من هذه المسؤولية وذلك بنصه صراحة على ذلك في المادة(65 مكرر 14) بقولها :" ...دون أن يكونوا مسؤولين جزائيا...". ويمتد هذا الإعفاء لظروف أمنية للمتسرب حتى بعد انقضاء المهلة المحددة في رخصة التسرب، وفي حالة عدم تمديدها أو في حالة تقرير وقف العمليّة، بشرط ألاّ يتجاوز ذلك مدة أربعة (4) أشهر سواء من تاريخ انقضاء المدة المحددة في الإذن أو من تاريخ صدور قرار وقفها من قبل القاضي الذي رخص بإجرائها.

وحتى تحقق عمليّة التسرب الأهداف المنشودة منه، ينبغي أن تتمّ بكل سريّة تامّة حتى يكون المتسرب في مأمن من انكشاف هويّته الحقيقيّة من قبل المجرمين، لذلك منحه المشرع نوعا من الحماية الجنائيّة، حيث قرّر عقوبة الحبس من سنتين(2) إلى خمس(5) سنوات وبغرامة من 50.000دج إلى 200.000دج لكل من يكشف هويّة ضباط أو أعوان الشرطة القضائيّة.

وإذا تسبب الكشف عن الهويّة في أعمال عنف أو ضرب وجرح على أحد هؤلاء الأشخاص أو أزواجهم أو أبنائهم أو أصولهم المباشرين فتكون العقوبة الحبس من خمس(5) سنوات إلى(10) سنوات والغرامة من 200.000 دج إلى500.000 د ج .

وإذا تسبب هذا الكشف في وفاة أحد هؤلاء الأشخاص فتكون العقوبة الحبس من عشر(10) سنوات إلى عشرين(20) سنة والغرامة من 500.000دج إلى1.000.000دج دون الإخلال، عند الاقتضاء بتطبيق أحكام الفصل الأول من الباب الثاني من الكتاب الثالث من قانون العقوبات.

وينبغي الإشارة في هذا المقام أن المشرع أدرج قواعد موضوعيّة والخاصة بالقواعد القانونية المتعلقة بالتجريم والعقاب ضمن القواعد الإجرائية و المتمثلة في مجموعة من القواعد التي تنظم وسائل التحقيق من وقوع الجريمة ومحاكمة مرتكبيها وتوقيع الجزاء الجنائي عليهم، لذلك ينبغي على المشرع أن ينقل الأحكام الخاصة بالقواعد الموضوعية إلى قانون العقوبات

حتى يكون لنا نظام قانوني جنائي منتظم ولا يلتبس على القاضي عند تطبيقه لإحدى هذه العقوبات.

وفي نهاية الفصل الخاص بإجراء التسرب قام المشرع بتكييف عمل المتسرّب على أنه شاهد حيث نص في المادة(65 مكرر 18)على أنّه :" يجوز سماع ضابط الشرطة القضائية الذي تجرى عمليّة التسرب تحت مسؤوليته دون سواء بوصفه شاهدا عن العمليّة.

ثانيًا: الشهادة في الجريمة الالكترونية

تُعرف الشهادة بصفة عامة بأنّها: "الأقوال التي يدلي بها غير الخصوم أمام سلطة التحقيق أو القضاء بشأن جريمة وقعت سواء كانت تتعلق بثبوت الجريمة وظروف ارتكابها وإسنادها إلى المتهم أو براءته منها" [1].

وتعدّ الشهادة من أقدم وأبرز وسائل الإثبات والحصول على الأدلة، حتّى أنّه لا يخلو منها تشريع إجرائي على مدار تاريخ القانون الجنائي[2]، فلها أهميّة بالغة في ميدان الإثبات، ذلك أنّ الجريمة ليست تصرفا قانونيا بل عمل غير مشروع يحدث فجأة و لا يتيسر عادة إثباته بالكتابة، بل يجتهد الجاني في التكتّم عند ارتكابه و يحرص اخفائه عن الناس، لذلك قال بنثام (Bentham) أنّ "الشهود هم عيون القضاء وأذانها [3]. وكثيرا ما يكون للشهادة أثناء جمع الاستدلالات أو التحقيق الابتدائي أكبر الأثر في القضاء بالإدانة أو بالبراءة، لأنّ الأقوال التي تتضمّنها قد أدلي بها فور وقوع الحادث قبل أن تمتدّ يد العبث وقبل أن يطول عليها الوقت فتضعف معالم الوقائع التي تنصب عليها [4].

ولا تقل الشهادة أهمية في الجريمة الالكترونية عن باقي الإجراءات في الحصول على الدليل الالكتروني، فالقاعدة العامة تقتضي بأن يلتزم الشاهد بالإفضاء بما يعلمه من معلومات

---

[1] د/ إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتورا، كلية الحقوق، جامعة القاهرة، 1980، ص 30.

[2] نظّم قانون الإجراءات الجنائية المصري الإثبات بشهادة الشهود في مرحلة التحقيق الابتدائي في الفصل السادس من الباب الثالث من الكتاب الأول من قانون الإجراءات الجنائية تحت مسمى" **في سماع الشهود** " وذلك في المواد من (110ــ 122) و في مرحلة المحاكمة تمّ تنظيم الشهادة في الفصل السابع تحت مسمى " **في الشهود و الأدلة الأخرى**" من الباب الثاني من الكتاب الثاني من الإجراءات الجنائية، وقد تمّ تنظيم شهادة الزور في قانون العقوبات المصري في الباب السادس من الكتاب في المواد(294ــ 301) " **شهادة الزور و اليمين الكاذبة**".

[3] أحمد شوقي الشلقاني، المرجع السابق، ص 247.

[4] د/ أيمن فاروق عبد المعبود حمد، الإثبات الجنائي بشهادة الشهود في الفقه الجنائي الإسلامي والقانون الجنائي الوضعي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2004، ص 81 .

بخصوص واقعة الجريمة و الفاعلين فيها، والإدلاء بكل ما يفيد في كشف الحقيقة من وقائع أخرى، وهو ما حدث فعلا في قضية (Broderbund) حيث شهد فيها الشهود بأن مبرمجي " يونيسون" قد طلب منهم نسخ برمجية "برودرباند" إلاّ أنهم قاموا ذلك بإهمال[1]. ومن خلال هذه القضية يتّضح لنا بأنّ الشاهد في الجريمة الالكترونية يختلف من حيث صفته عن غيره من الشهود في الجرائم التقليدية، غالبا ما يكون من أصحاب المعرفة التقنية للنظام المعلوماتي وذلك بحكم عملهم، ولا يقصد من ذلك أن يكون الشاهد خبيرا، بل كلاهما يختلفان عن بعضهما البعض، حيث يقدّم هذا الأخير تقارير وآراء توصّل إليها بتطبيق قوانين علميّة أو أصول فنية، أمّا الشاهد يقدّم إلى القاضي معلومات حصلها بالملاحظة الحسية[2].

وسنبين في ما يلي تحديد المقصود من الشاهد في الجريمة الالكترونية، التزاماته ومدى حدودها في الجريمة الالكترونية.

أ ـ المقصود بالشاهد في الجريمة الالكترونية :

الشاهد في الجريمة الالكترونية هو الفنّي صاحب الخبرة والتخصّص في تقنية الحاسب وشبكات الاتّصال الذي تكون لديه معلومات جوهرية لازمة لولوج نظام المعالجة الآلية للبيانات إذا كانت مصلحة التحقيق تقتضي التنقيب عن أدلة الجريمة داخله[3]. وهي تشمل بهذا المفهوم عدّة طوائف أهمّها: مشغلو الحاسوب، خبراء البرمجة، المحللون، مهندسو الصيانة، مديرو النظم، وسنحاول تفصيل ذلك فيما يلي:

1ـ القائم على تشغيل الحاسب الآلي: وهو المسؤول عن تشغيل جهاز الحاسب الآلي والمعدّات المتّصلة به، ويجب أن تكون لديه خبرة كبيرة في تشغيل الجهاز واستخدام لوحة المفاتيح في إدخال البيانات، كما يجب أن تكون لديه معلومات عن قواعد كتابة البرامج[4].

2ـ المبرمجون: وهم الأشخاص المتخصصون في كتابة البرامج ويمكن تقسيمهم إلى فئتين:

- الفئة الأولى: هم مخططو برامج التطبيقات.
- الفئة الثانية: هم مخططو برامج النظم.

---

(1) د/ عمر أبوبكر بن يونس، المرجع السابق، ص 951 .

(2) د/ محمود نجيب حسني، المرجع السابق، رقم 927، ص 847. وانظر أيضا: نقض جنائي جلسة 1979/4/2، مجموعة أحكام النقض، سنة 230 رقم 290، ص 426.

(3) د/ هلالي عبد الله أحمد، التزام الشاهد بالإعلام في الجريمة المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006، ص 23.

(4) انظر في ذلك: د/.محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، مطابع المكتب المصري الحديث، 1991.ص 23 وما بعدها .

حيث يقوم مخططو برامج التطبيقات بالحصول على خصائص ومواصفات النظام المطلوب من محلل النظم ثم يقوم بتحويلها إلى برامج دقيقة وموثقة لتحقيق هذه المواصفات، أمّا مخطّطو برامج النظم فيقومون باختبار وتعديل وتصحيح برامج نظام الحاسب الداخلية أي انه يقوم بالوظائف الخاصة بتجهيز الحاسب بالبرامج والأجزاء الداخلية التي تتحكم في وحدات الإدخال والإخراج ووسائط التخزين بالإضافة إلى إدخال أي تعديلات أو إضافات لهذه البرامج.

3ـ **المحللون:** المحلل وهو الشخص الذي يحلل الخطوات ويقوم بتجميع بيانات نظام معين، ودراسة هذه البيانات ثم تحليل النظام أي تقسيمه إلى وحدات منفصلة واستنتاج العلاقات الوظيفية من هذه الوحدات، كما يقوم بتتبع البيانات داخل النظام عن طريق ما يسمّى بمخطط تدفق البيانات واستنتاج الأماكن التي يمكن ميكنتها بواسطة الحاسب [1].

4ـ **مهندسو الصيانة والاتصالات**: وهم المسؤولون عن أعمال الصيانة الخاصة بتقنيات الحاسب بمكوناته وشبكات الاتصال المتعلقة به.

5ـ **مديرو النظم:** وهم الذين يوكّل لهم أعمال الإدارة في النظم المعلوماتية.

بالإضافة إلى هذه الفئات، هناك أشخاص آخرون يعدّون بمثابة شهود في الجريمة الالكترونية، وهذه الفئة لها دور كبير في توصيل المستهلك إلى شبكة الانترنت، من بينهم : مقدمو الخدمات الوسطية في مجال المعلوماتية والانترنت، أيضا متعهدو الوصول ومتعهدو الإيواء ومسئولو المنتج ومسئولو ناقل المعلومات ومسئولو متعهد الخدمات، كذلك مورّد المعلومات و مؤلف الرسالة [2].

ب ـ التزامات الشاهد المعلوماتي (الالكتروني):

إذا كان يتعيّن على الشاهد المعلوماتي أن يقدّم إلى سلطات التحقيق ما يحوزه من معلومات جوهرية لازمة للولوج في الحاسبات و المواقع التي تحتوي على المعلومات التي تشكّل جريمة بحثا عن أدلة تثبتها، فالسؤال الذي ينبغي طرحه في هذه الحالة يتمثل في الآتي: **هل يلتزم الشاهد المعلوماتي بأن يتعاون مع سلطة التحقيق كأن يقوم مثلا بعمليات معينة على الجهاز لكي يساعد العدالة، خاصة وأنّ المؤتمر الدولي الخامس عشر للجمعية العامة لقانون العقوبات و الذي عقد في ريودي جانيرو بالبرازيل في الفترة من 4ـ 9 سبتمبر فيما يتعلق بالقانون الإجرائي أوصى بواجب التعاون الفعّال من جانب المجني عليهم و الشهود**

---

(1) د/ هلالي عبد الله أحمد، المرجع السابق، ص 24.

(2) لمزيد من التفصيل حول هذه الفئات أنظر: د/ عبد الفتاح بيومي حجازي، المرجع السابق، ص38 و ما بعدها.

وغيرهم من مستخدمي تكنولوجيا المعلومات ؟ فهل يقصد بالتعاون الفعّال من جانب الشاهد قيامه بطبع الملفات المخزنة في ذاكرة الحاسوب أو الإفصاح عن كلمات المرور السرية أو الكشف عن الشفرات الخاصة بالبرامج المختلفة؟

إن الإجابة على هذه التساؤلات لها أهميتها حيث أنّ الخبير المنتدب من الجهة القضائية قد لا يمكنه معرفة الأساليب الفنية التي يمكن إتباعها للكشف عن أدلة تفيد في كشف الحقيقة، وقد لا يعلمها إلاّ هذا الشاهد مثل كلمة المرور و البرامج المستخدمة و التي استعان بها المتهم في ارتكاب الجريمة الالكترونية.

ـ يتنازع الفقه المقارن اتجاهين مختلفين بصدد مدى إلزام الشاهد في الجريمة الالكترونية على تقديم دليل فنّي، و ذلك كما يلي:

الاتجاه الأول: يرى أنصار هذا الاتجاه أنّه ليس من واجب الشاهد ـ وفقا للالتزامات التقليدية للشهادة ـ أن يقوموا بطباعة البيانات المخزنة في ذاكرة الحاسوب أو تحليل ذاكرة النظام المعلوماتي ليكشف له عن آثار بعض البيانات. فهذا البحث يدخل في اختصاص الخبير القضائي[1]. ويجد هذا الاتجاه تجسيده التشريعي و الفقهي في كلّ من ألمانيا [2] و تركيا [3].

وعلى عكس الاتجاه الأول يرى أنصار **الاتجاه الثاني**، أنّ من بين الالتزامات التي يتحمّل بها الشاهد القيام بطبع ملفات البيانات أو الإفصاح عن كلمات المرور أو الشفرات الخاصة بالبرامج المختلفة. ومن التشريعات التي تفرض واجب التعاون على الشاهد في مجال الجريمة الالكترونية القانون الانجليزي الصادر عام 1984 بشأن البوليس والأدلة الجنائية، حيث يعطي للمحققين الحق في أن يطلبوا من الغير تمكينهم من الدخول إلى المعلومات المخزنة في الحاسب الآلي أو الاطلاع عليها أو قراءتها[4].

ويتيح مشروع قانون الحاسب الآلي في هولندا لسلطات التحري والتحقيق إصدار الأمر للقائم بتشغيل النظام لتقديم المعلومات اللازمة لاختراقه والولوج إلى داخله، كالإفصاح عن كلمات المرور السرية والشفرات الخاصة بتشغيل البرامج المختلفة. وإذا وجدت بيانات مشفرة

---

(1) د/ جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دراسة مقارنة، دار النهضة العربية، القاهرة، 2002، ص 106.

(2) Mohrenschloager (Manfred): Computer crimes and other crimes against information technology in Germany "R.I.D.P. 1993. P. 351.

(3) Erman (Sahir) "les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie" R.I.D.P. 1993، p.64.

(4) Verguchi Pascal، op.cit،N°321،p.398 et 399.

مشار إليه عند: د/ جميل عبد الباقي الصغير، المرجع السابق، ص 107.

او مرمّزة داخل ذاكرة الحاسب وكانت مصلحة التحقيق تستلزم الحصول عليها، يــتمّ تكليــف القائم على تشغيل النظام المعلوماتي بحلّ رموز هذه البيانات(المادة 125-k)[1].

وتجدر الإشارة إلى أنّ بعض الفقهاء في فرنسا يؤيدون هذا الاتجاه، ويبــرّرون مــوقفهم على أساس أنّ المشرع الفرنسي طالما لم ينظّم هذه المسألة فانّه لا مناص من تطبيق القواعــد العامة في الشهادة، ومن ثمّ فان الشهود الذين تقع على عاتقهم الالتزام بالشهادة يكونون مكلفين بالكشف عن كلمات المرور السريّة التي يعرفونها، وشفرات تشغيل البرامج، باستثناء حــالات المحافظة على سر المهنة فإنّهم يكونون في حلّ من هذا الالتزام[2].

وفي إطار الموازنة بين الرأيين، ينبغي علينا أولاً تبيان الالتزامات التي أوجبها القــانون على الشاهد بصفة عامة من جهة، ومن ثمّ نرجح أياً من هذه الاتجاهات أصوب مــن جهــة ثانية.

ـ التزامات الشاهد:

يتحمّل الشاهد ثلاث التزامات أساسيّة هي: الحضور أمام الجهة التي اســتدعته، حلــف اليمين و أخيرا الإدلاء بالشهادة.

1ـ **حضور الشاهد:** موضوع هذا الالتزام هو حظور الشاهد بنفسه في المكان والوقت المحدّدين للاستماع إلى شهادته، ثمّ البقاء فيه حتّى يؤذن له بالانصراف[3]، ويكون ذلك بناء على تكليف بالحضور يُعلن إليهم بواسطة أحد المحضرين أو أحد رجال الضبط، والإخلال بهذا الالتــزام يعاقب عليه بإحدى الطرق التالية:

ـــ أول عقاب يتمثّل في الحكم على الشاهد المتخلّف عن الحضور بغرامة وذلك بعــد ســماع أقوال النيابة العامة، لا تتجاوز قيمتها عشر جنيهات في المخالفات و ثلاثين جنيها في الجــنح وخمسين جنيه في المخالفات، وهذا العقاب لا يوقع على الشاهد إلاّ أثناء المرحلة القضائية من الدعوى الجنائية المادة (1/279) من قانون الإجراءات الجنائية المصري، ويمكن إعفاء الشاهد المتخلّف عن هذه الغرامة من قبل المحكمة وذلك إذا حضر سواء بناء على تكليفه بالحــضور مرّة ثانية أو من تلقاء نفسه، وأبدي أعذارا مقبولة، وذلك بعد سماع أقوال النيابة العامة المادة

---

[1] د/ هشام محمد فريد رستم، المرجع السابق، ص 85.

[2] Dr.Jacques francillon, "les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France",R.I.D.P. 1993, p. 309.

[3] د/ محمود نجيب حسني، المرجع السابق، ص 448.

(1/280) من ذات القانون[1]، وإذا تخلّف رغم تكليفه بالحضور للمرة الثانية و تغريمه، جاز للمحكمة أن تحكم عليه للمرّة الثانية بغرامة لا تتجاوز ضعف الحد الأقصى المقرر كجزاء للتخلّف بعد تكليفه لأوّل مرّة، وللمحكمة أن تأمر بالقبض عليه و إحضاره في نفس الجلسة أو في جلسة أخرى تؤجل إليها الدعوى المادة (2/280) من قانون الإجراءات الجنائية المصري.

ـ و العقاب الثاني يتمثّل في إجبار الشاهد على الحضور و لو اقتضى الأمر استعمال القوة العموميّة المادة (2/97) من قانون الإجراءات الجزائية الجزائري.

ـ أمّا الإجراء الأخير، هو ليس عقابا في حقيقة الأمر، إذ يتمثل فقط في تأجيل النظر في الدعوى لإعادة تكليفه بالحضور، و يتحمّل الشاهد المتخلّف جميع المصاريف التي تنجر عن هذا التأخير، خاصة إذا تعلق الأمر بمحكمة الجنايات .

و إذا تقدّم الشاهد بأعذار مقبولة عن عدم إمكانية الحضور، فللمحكمة أن تنتقل إليه وتسمع شهادته بعد إخطار النيابة العامة و باقي الخصوم، والذين لهم أن يحضروا بأنفسهم أو بواسطة وكلائهم، وأن يوجّهوا للشاهد الأسئلة التي يرون لزوم وقوعها إليه المادة (281) من قانون الإجراءات الجنائية المصري.

2 **ـ حلف اليمين**[2]: ألزم المشرّع الشاهد أن يحلف اليمين قبل أداءه الشهادة، وذلك كضمانة تضفي عليها الثقة كي تكون دليلا يستمد منه القاضي اقتناعه، و تعطي لها قيمتها القانونية من جهة، ومن جهة أخرى تجلب هذه الشكليّة انتباه الشاهد إلى خطورة ما سيدلي به، حيث تجعله حريصا على قول الحق. وقد نصّت على هذا الالتزام المادة (283) من قانون الإجراءات الجنائية المصري[3]، كما نصت المادة (119) من قانون الإجراءات الجنائية المصري على وجوب حلف اليمين القانونية في مرحلة التحقيق، ولكن لا يحلف الشهود اليمين في مرحلة الاستدلال المادة (2/29) من ذات القانون.

---

[1] د/ محمد زكي أبو عامر، الإجراءات الجنائية، دار الجامعة الجديدة، الإسكندرية، الطبعة السابعة، 2002، ص 965. وانظر أيضا: د/ مأمون محمد سلامة، قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام النقض، الجزء الثاني، الطبعة الثانية، 2005، بدون دار النشر، ص 901.

[2] يقصد باليمين " إشهاد الله سبحانه وتعالى أنّ الحقيقة كما يقول حالفها"، ويعرفها البعض " أن يتخذ الله سبحانه و تعالى رقيبا على صدق شهادته ويعرض نفسه لغضبه و انتقامه إن كذب فيها". انظر بالترتيب: د/ جابر علي مهران، واجب القاضي بعد سماع الدعوى والإثبات في الفقه الإسلامي، مجلة الدراسات القانونية، كلية الحقوق، جامعة أسيوط، العدد الخامس عشر، يونيو 1993، ص 87. وانظر أيضا:
Roger Merle et Andre Vitu,op. cit, n' 938, p. 157.

[3] تنص المادة (283) من قانون الإجراءات الجنائية المصري على أنّه "يجب على الشهود الذين بلغت سنّهم أربع عشرة سنة أن يحلفوا يمينا قبل أداء الشهادة على أنّهم يشهدون بالحق و لا يقولون إلاّ الحق".

وإذا كان المشرع الجزائري حدّد صيغة اليمين وذلك حسبما جاءت واردة في المادة (93/ 2) من قانون الإجراءات الجزائية الجزائري وهي كالتالي: "أقسم بالله العظيم أن أتكلم بغير حقد و لا خوف و أن أقول كل الحق و لا شيء غير الحق". وذلك بخلاف المشرع المصري فلم يبيّن صيغة اليمين، ولكن هذا اللفظ الأخير يتضمّن في ذاته معنى الدّين وأن يكون القسم بالله[1]، أمّا بالنسبة للمشرع الفرنسي تختلف صيغة اليمين باختلاف المحاكم، فهي أمام محكمة الجنايات طبقا للمادة (3/331) من قانون الإجراءات الجنائية الفرنسي كالتالي: "أتكلم بدون حقد و بدون خوف و أقول كل الحق و لا شيء غير الحق"[2]، و الطيغة أمام محاكم الجنح والمخالفات و قضاة التحقيق طبقا للمواد (103ــ 446ــ536) وهي كالآتي: " أنّ الشاهد يقول كل الحق ولا شيء غير الحق"، وتجدر الإشارة أنّ صيغة اليمين في القانون الفرنسي حتميّة، و جزاء مخالفتها البطلان.

ــ ويجب على المحكمة أو المحقق أن يثبت في محضر الدعوى حلف الشاهد لليمين، ويترتّب على مخالفة هذا الإجراء بطلان الشهادة عند كل من التشريعين الفرنسي و الجزائري[3]، بخلاف الحال في التشريع المصري فلا يترتب على إغفاله البطلان[4].

ومن الملاحظ أنّ الالتزام بأداء اليمين من النظام العام، فلا يمكن للشاهد الامتناع عن أدائها وإلاّ فإنّه يعامل معاملة الممتنع عن الإدلاء بالشهادة[5]. كما لا يمكن للشاهد أن يطلب من القاضي إعفاءه من أداء اليمين.

---

[1] د/ أيمن فاروق عبد المعبود حمد، المرجع السابق، ص 142.

[2] Article 331، alinéa 3 du C.P.P.F dispose que:" Avant de commencer leur déposition, les témoins prêtent le serment "**de parler sans haine et sans crainte, de dire toute la vérité, rien que la vérité**".

[3] أقرّت الغرفة الجنائية لدى المحكمة العليا أنّ عدم الإشارة إلى أداء اليمين في محضر المرافعات أو في الحكم يؤدي إلى نقض ها الأخير. المحكمة العليا، غ. ج: 22أكتوبر 1968، مجموعة الأحكام ص 386. كما أقرّت نفس الغرفة : أنّه ليس من الضروري ذكر اليمين بأكملها، بل يكفي أن يثبت في محضر المرافعات أو في الحكم أنّ الشاهد حاف اليمين على أن يقول الحق". انظر: المحكمة العليا، غ. ج: 26 نوفمبر 1985، المجلة القضائية العدد الأول، لسنة 1990، ص 242. وهذا خلافا لما أكّدته محكمة النقض الفرنسية، من أنّه لا ينبغي تبديل صيغة اليمين الواردة بالنص حذفا أو إضافة. انظر

Cass،Crim 20 septembre. 1967، Bull n' 336، disponible en ligne à l'adresse suivante:http\\www.couredecassation.fr.

[4] د/ محمود نجيب حسني، المرجع السابق، ص 452.

[5] فتطبق عليه المادة (2/97) من قانون الإجراءات الجزائية الجزائري، وتقابلها المادة (284/ 1) من قانون الإجراءات الجنائية المصري.

3 ـ **الالتزام بالإدلاء بالشهادة:** ويعدّ من أهمّ الالتزامات المفروضة على الشاهد، فهو جوهر مهمته، وينطوي هذا الالتزام في حقيقة الأمر على واجبين اثنين يتحمّلهما الشاهد:

أ ـ **الواجب الأوّل:** الالتزام بالتكلّم، فالشاهد على عكس ما هو عليه المتّهم، لا يمكنه أن يسكت، فيجب عليه أن يدلي بشهادته، إلاّ إذا كان الشخص المراد الاستماع إلى شهادته ملتزم قانونا بالسر المهني كالأطباء و المحامين و غيرهم ممّن لهم مبرر قانوني لذلك. أما جزاء الإخلال بهذا الواجب فإنّه الإدانة بغرامة كالتالي:

ـ **في التشريع الجزائري** : من 1000إلى 10.000دج، لكن العقوبة تكون أكثر قساوة في حالة ما إذا كان الشخص يعرف مرتكبي جناية أو جنحة و يرفض الإجابة عن الأسئلة الموجّهة إليه في هذا الشأن.

ـ **في التشريع المصري** : لا تزيد الغرامة على عشرة جنيهات في المخالفات، و في مواد الجنح و الجنايات بغرامة لا تزيد عن مائتي جنيها، و إذا عدل الشاهد عن امتناعه قبل إقفال باب المرافعة يعفى من العقوبة المحكوم بها عليه كلّها أو بعضها المادة(119ـ 284) إجراءات جنائية مصري .

ب ـ **الواجب الثاني:** واجب قول الحقيقة، فلا يمكن للشاهد أن يساهم في إظهار الحقيقة إلاّ إذا كانت شهادته نزيهة غير كاذبة، ومن هنا لا يكف أن يمتثل و يحلف اليمين بل إنّه ملتزم بقول الحقيقة. لذلك فإنّ الإخلال بواجب الحقيقة يعاقب عليه جنائيّا، وقد ورد النّص على العقاب على شهادة الزور في المواد (332) من قانون العقوبات الجزائري، والمواد من(294 إلى 298) قانون العقوبات المصري.

وعلى ذلك نرى أنّه وفقا للقواعد السابقة الذكر أنّ الشاهد لا يلتزم إلاّ بذكر ما يعلمه عن الجريمة و لا يجوز إجباره على القيام بعمل معيّن، ونلاحظ أنّ المادة 284 من قانون الإجراءات الجنائية المصري تنصّ على أنّه " إذا امتنع الشاهد عن أداء اليمين أو الإجابة في غير الأحوال التي يجيز له القانون فيها ذلك، حكم عليه..."، ومعنى ذلك أنّ الشاهد يلتزم بالإجابة عن أسئلة توجهها المحكمة له و ليس للمحكمة أن تلزمه بالقيام بعمل معين، وفي ذلك تقول محكمة النقض المصريّة أنّ الشهادة هي تقرير شخص لما يكون قد رآه أو سمعه بنفسه أو أدركه على وجه العموم بحواسه[1]، و بالمثل فإنّ المادة (331) من قانون الإجراءات الفرنسي تحدّد واجبات الشاهد في الشهادة بخصوص الوقائع المسندة إلى المتهم أو بخصوص شخصية هذا الأخير أو أخلاقياته، لذلك ليس من واجب الشاهد في الجريمة الالكترونيّة طبع ملفات البيانات المخزّنة في ذاكرة الحاسوب، أو الإفصاح عن كلمات المرور السريّة

---

[1] نقض 15 يوليو سنة 1964، س15 ، ق رقم 98، ص 493.

أو الكشف عن الشفرات المدوّنة بها الأوامر الخاصة بتنفيذ البرامج، إذ أنّ هذا الالتزام يزيد عن نطاق الشهادة ، لذلك ينبغي أن يكون هناك تدخّل تشريعي عن طريق وضع نصوص قانونيّة خاصة لكي تفرض على الشاهد واجب التعاون مع الجهة القضائية في أثناء التحقيقات والمحاكمة. وفي هذا الإطار يقول الفقيه الشيلي (Kunsemuller) " أنّه في غياب نصوص صريحة، لا مجال للحديث عن وسيلة قانونية لإلزام أشخاص معنيين بالكشف أو الإفصاح عن كلمات السر أو طبع ملفات بيانات مختزنة في ذاكرة الحاسب، فضلا عن أنّه يجب أن يكون في الاعتبار أنّ مثل هذا الإفصاح قد تتحقّق به جريمة إفشاء الأسرار.." [1].

وتجدر الإشارة في هذا الصدد أنّه نتيجة قصور أحكام الشهادة في الحصول على الدليل الالكتروني، يرى بعض الفقهاء[2] ضرورة البحث عن وسيلة قانونية جديدة تحقّق ما لم تستطع فكرة الالتزام بأداء الشهادة أن تؤدّيه، وهذه الوسيلة هي" الالتزام بالإعلام في الجريمة المعلوماتية" [3]، وقد تستعمل بعض الدول وسائل للضغط على الشهود بهدف حملهم على التعاون الايجابي مع سلطات التحقيق، حيث يُسأل الشاهد الذي يخفي الشفرة أو كلمة السرّ أو الذي يعطي أوامر خاطئة عن جريمة شهادة الزور لأنّه يعوق سير العدالة، أو يُسأل باعتباره شريكا في الجريمة موضوع المحاكمة [4].

ثالثا: الخبرة التقنية

الخبرة القضائية عموما هي الاستشارة الفنيّة التي يستعين بها القاضي أو المحقق لمساعدته في تكوين عقيدته نحو المسائل التي يحتاج تقديرها إلى معرفة أو دراية علميّة خاصة لا تتوافر لديه[5] فهي وسيلة من وسائل الإثبات التي تهدف إلى كشف بعض الدلائل أو الأدلة أو تحديد مدلولها بالاستعانة بالمعلومات العلميّة والفنيّة والتي لا تتوافر سواء لدى المحقّق أو القاضي.

---

[1] Carlos Kunsemuller, Computer crimes and other crimes against information technology in Germany, "R.I.D.P. 1993. P. 256.

[2] دكتور: هلالي عبد الله أحمد

[3] لمزيد من التفصيل حول هذا الموضوع أنظر: د/ هلالي عبد الله أحمد، المرجع السابق، ص 25 وما بعدها.

[4] د/ جميل عبد الباقي الصغير، المرجع السابق، ص 110.

[5] د/ أمال عثمان، الخبرة في المسألة الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1964، ص 68 وما بعدها. وانظر أيضا: د/ عادل حافظ غانم، الخبرة في مجال الإثبات الجنائي، بحث بمجلة الأمن العام، العدد 43، سنة 1968، ص 19 وما بعدها.

وتقدّم الخبرة عونا ثمينا لجهة التحقيق والقضاء ولسائر السلطات المختصّة بالـدعوى الجنائيّة في أداء رسالتها، فبدونها يتعذّر الوصول إلى الرأي السديد بشأن المسائل الفنيّة التـي يكون على ضوئها كشف جوانب الحقيقة المبنيّة على الأصول والحقائق العلميّة[1]. لذا فقد اهتمّ المشرع في كلّ من الجزائر ومصر بتنظيم أعمال الخبرة، حيث أجـاز قـانون الإجـراءات الجنائية الجزائري والمصري الاستعانة بالخبراء لكل من مأمور الضبط القـضائي والنيابـة العامة وقاضي التحقيق، ولم يحظر كل من القانونين على المحاكم أن تستعين بالخبراء، فيجوز لها أن تعيّن خبيرا واحدا أو أكثر سواء من تلقاء نفسها أو بناء على طلب الخصوم[2].

وإذا كان للخبرة تلك الأهميّة في الجرائم التقليديّة فـإنّ أهميّتهـا تـزداد وتـصبح ضروريّة بل وحتميّة في اشتقاق الأدلة الالكترونيّة لإثبات الجرائم الالكترونية، حيث تتعلّـق بمسائل فنيّة آية في التعقيد ومحل الجريمة فيها غير مادي، والتطوّر فـي أسـاليب ارتكابهـا سريع ومتلاحق، ولا يكشف غموضها إلاّ متخصّص وعلى درجة كبيرة من التميّز في مجـال تخصصه، فإجرام الذكاء والفن لا يكشفه ولا يفلّه إلا ذكاء وفنّ مماثلين وذلك من خلال الخبرة التقنيّة، والتي تعدّ أقوى مظاهر التعامل القانوني أو القضائي مع ظاهرة تكنولوجيا المعلومات والانترنت، فهي تؤدي دورا لا يستهان به إزاء نقص المعرفة القضائيّة الشخـصية لظـاهرة الانترنت[3]، ويظهر ذلك جليّا في فشل جهات التحقيق جمع الأدلة الالكترونيّة، بل أنّ المحقق في كثير من الأحيان يدمّر الدليل الفنّي كنتيجة خطأ أو إهمال في التعامل معه. ولذلك بـات من الضروري الاستعانة بالخبرة التقنيّة في مجال الجريمة الالكترونيّة، وهذا ما حدث بالفعل في قضيّة اتحاد الطلاب اليهود بباريس حيث التمس اتحاد طلاب اليهود من القاضي أن يندب خبيرا تكون مهمّته تحديد ما إذا كانت هناك إجراءات مناسبة من شأنها منـع الـدخول إلـى المواقع التي تحتوي مقالات مناهضة لليهود، فضلا عن إمكانية تحديد مـسار أمنـي وذلـك باستخدام الفلترة[4].

والخبرة التقنية في أغلب التشريعات شأنها في ذلك شأن الخبرة القضائية في الجرائم التقليدية من حيث القواعد القانونية التي تحكم الخبرة عموما سواء من خلال اختيار الخبـراء

---

(1) د/ سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، ص 440.

(2) انظر المواد (143 إلى 156) إجراءات جزائية جزائري، والمواد (29و85 ـ 89 و292) إجراءات جنائية مصري.

(3) د/ عمر بن يونس، المرجع السابق، ص 1031.

(4) انظر تفاصيل هذه القضية على الموقع التالي :

http://www.internet-juridique.com/control.php

أو من حيث عمليات الخبرة في حدّ ذاتها باختلاف الأمور الفنيّة التي تحكم عمل الخبير التقني، إلاّ أنّ هناك بعض التشريعات نظّمت أعمال الخبرة في مجال الجرائم الالكترونيّة مثل القانون البلجيكي الصادر في(23 نوفمبر سنة 2000)[1].

وقد نصّت المادة(88) من القانون البلجيكي المذكور على أنّه "يجوز لقاضي التحقيق، وللشرطة القضائية أن يستعينا بخبير ليقدم وبطريقة مفهومة المعلومات اللازمة عن كيفية تشغيل النظام، وكيفيّة الدخول فيه، أو الدخول للبيانات المخزونة أو المعالجة أو المنقولة بواسطته، ويعطي القانون كذلك لسلطة التحقيق أن تطلب من الخبير تشغيل النظام أو البحث فيه أو عمل نسخة من البيانات المطلوبة للتحقيق أو سحب البيانات المخزنة أو المحمولة أو المنقولة، على أن يتمّ ذلك بالطريقة التي تريدها جهة التحقيق"[2].

والإشكال المطروح هنا هو: **هل يلتزم القاضي دائما برأي الخبير التقني باعتباره رأيا فنيّا محضا، أم أنّه مازال للقاضي الفسحة في تلك الدعوى في أن يطرح رأي الخبير ويعتبر نفسه الخبير الأعلى؟**

وفي ظل دراستنا للخبرة التقنيّة، ارتأينا التطرق إلى هذا النوع المستحدث من الخبرة، من خلال الإشارة إلي القواعد القانونية والفنيّة التي تحكم أعمال الخبير التقنيّ، وذلك فيما يلي:

أ ـ القواعد القانونيّة التي تحكم الخبرة التقنيّة: وسنتناول من خلالها طرق اختيار الخبراء، وواجبات الخبير التقني فضلا عن تحديد مدى حجيّة تقرير الخبير، وذلك من خلال النقاط التالية:

1ـ اختيار الخبراء: حدّد كل من المشرّع الجزائري والمصري طرق اختيار الخبراء، حيث نصّت أحكام قانون الإجراءات الجزائيّة الجزائري على أنّه:" يختار الخبراء من الجدول الذي تعدّه المجالس القضائيّة بعد استطلاع رأي النيابة العامة. وتحدّد الأوضاع التي يجري بها قيد الخبراء أو شطب أسماءهم بقرار من وزير العدل. ويجوز للجهات القضائيّة بصفة استثنائيّة أن تختار بقرار مسبّب خبراء ليسوا مقيّدين في أي من هذه الجداول"[3] وذلك كحالة عدم وجود الخبرة المطلوبة ضمن هذه الجداول. أمّا بالنسبة للتشريع المصري، فلم يعد هناك خبراء الجداول فقد أصبح جزءا من التاريخ، وذلك بعد ما قفل المرسوم بقانون رقم(96 لسنة 1952) الخاص بتنظيم الخبرة أمام جهات القضاء هذه الجداول[4]، ونصّ في مادته الثانيّة على

---

[1] Meunier (C), op.cit, p. 611.

[2] Meunier (C)، ibid، p. 681.

[3] مادة (144) إجراءات جزائيّة جزائري.

[4] وفي ذلك يرى الفقه أن المشرع المصري أحسن فعلا في المرسوم بقانون رقم 96 لسنة 1952 من اتجاهه منذ صدوره إلى طرح نظام الجداول الثابتة، وأنه النظام الأولى بالتأييد لضمان الحيدة والكفاءة، فمرفق

أن يستمرّ الخبراء المقيّدون في جداول المحاكم في تاريخ صدوره في أعمالهم، كل منهم في القسم المدرج فيه، ولا يجوز أن يقيّد في هذه الجداول أحد بدلا ممن تخلو محالهم في أي قسم من الأقسام.

والآن بعد تصفية هذه الجدول لم يبق أمام القاضي سوى اختيار خبراء وزارة العدل ومصلحة الطب الشرعي والمصالح الأخرى التي يعهد إليها بأعمال الخبرة كإدارة تحقيق الشخصيّة ومصلحة الميكانيكا.. (المادة الأولى من المرسوم بقانون رقم 96 لسنة 1952)[1].

وقد ترك القانون لقاضي التحقيق حرية ندب خبير واحد أو خبراء متعدّدين(المادة 147) قانون الإجراءات الجزائيّة الجزائري، وهذا التعدد ضروري في مجال الخبرة التقنية، ذلك أنّه من الصعوبة وجود متخصّص منفرد له الدراية الكاملة بتقنيات الحاسوب ونظمه، حتّى وإن كان يملك القدرات الماليّة على الظهور بمظهر المتفرّد في مجال الخبرة القضائيّة، هذا من جهة .

ومن جهة أخرى، لم يحدّد المشرع طبيعة شخص الخبير سواء كان شخصا طبيعيّا أو شخصا معنويّا كمؤسسة متخصّصة تعمل في مجال المحاسبة مثلا، وان كان الواقع العملي للخبرة الاستعانة بالشخص الطبيعي، إلاّ انّه في مجال الجريمة الالكترونيّة يتعيّن الاستعانة بشركات ومنظمات أو مؤسسات متخصّصة، حيث تملك موارد ماديّة من برامج وأجهزة حديثة، وموارد بشرية من مهندسين متخصّصين في الحاسوب والانترنت، ومن أمثلة هذه الشركات، مختبر الخبرة والبحث عن البصمات (الآثار) المعلوماتية في فرنسا "Lerti"[2].

الخبراء كمرفق القضاء أو هو جزء منه أو مكمّل له، لكنّه ذات سمة علميّة أو كما يطلق عليه كثيرون هو قضاء علمي فنّي. انظر: د/ فتحي محمد أنور محمد عزت، دور الخبرة في الإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كليّة الحقوق، جامعة عين شمس، 2007، ص 189. وانظر أيضا: عبد الناصر محمد محمد فرغلي ود/ محمد عبيد سيف سعيد المسماري، المرجع السابق، ص 27.

(1) لمزيد من التفاصيل حول هذه الطوائف من الخبراء انظر: د/ سليمان مرقس، أصول الإثبات وإجراءاته في المواد المدنيّة في القانون المصري مقارنا بتقنينات سائر البلاد العربيّة، الطبعة الرابعة، دار النهضة العربيّة، 1986، ص 326 وما بعدها.

(2) Le laboratoire d'expertise et de recherche de traces informatique "Lerti" : تمّ إنشاء هذا المختبر سنة 2004من قبل اشتراك خمسة خبراء تقنية من أعلى مستوى في فرنسا، وهذا المختبر مختص في التحقيق الرقمي واستعادة البيانات والبحث عن الآثار المعلوماتية على جميع أنواع الوسائل المعلوماتيّة (كالقرص الصلب، مفاتيح USB وأجهزة المساعد الرقمي الشخص(PDA) ، البطاقات الذكيّة المصرفيّة وأيضا الهواتف المحمولة). وتمّ تعيين هذا المختبر كأوّل شخص معنوي في مجال الخبرة القضائية في فرنسا، حيث أدى هذا المختبر اليمين القانونيّة في 29 يناير، أمام محكمة استئناف Grenoble ، وتمّ تسجيله في قائمة جدول الخبراء. لمزيد من التعريف حول "Lerti"، انظر الموقع الخاص به.

www.Lerti.fr

وتجدر الإشارة في هذا الإطار أنّ بعض الفقه[1] يرى أنّه لا يشترط في الخبير المنتدب أن يكون متخرّجا من معاهد أو جامعات متخصّصة في دراسات الحاسوب والانترنـــت، بـــل يكفي اكتسابه مهارة وموهبة استعمال الحاسوب والانترنت والتعامل مع تقنيّة المعلومـــات، إذ أنّ أمهر مبرمجي نظم التشغيل حتّى الآن مثل (Bill Gates)، لم يكن تحصيله العلمي يتجاوز المرحلة الثانويّة، وذات الأمر ينطبق على عتاة الهكرة ومخترقي الأنظمة فـــإنّ أعمـــارهم لا تتجاوز مرحلة التعليم الثانوي.

وعلى ذلك، بالرغم من صحة قول الرأي السابق ــ إمكانية القضاء الاستعانة بخبير غير دارس ، إلاّ أنه يؤخذ عليه بأنه يتعارض مع الواقع القانوني، ذلك أنّه عادة ما يحرّر الخبير في نهاية أعمال الخبرة تقريرا، ويلزم هذا الأخير أن يكون متكاملا لعناصره الشكليّة والموضوعيّة[2]، وبالتالي لا يمكن لشخص ذي دراية فنيّة فحسب أن يُعدّ هذا التقرير. فضلا على أنّ هذا الرأي من شأنه جعل جميع أفراد المجتمع بمختلف الأعمار خبراء تقنيّة نتيجة الانتشار الواسع لمعرفة تقنية الحاسوب والانترنت في أواسط هذه المجتمعات.

2ـ واجبات الخبير التقني: تتمثل هذه الواجبات فيما يلي:

1ــ حلف اليمين: أوجب القانون[3] على الخبير حلف اليمين قبل أداء مأموريته، وإلاّ كان العمل باطلا، فهو إجراء جوهري قصد منه المشرع حمل الخبير على الصدق والأمانـــة فـــي عمله وبثّ الطمأنينة في آراءه التي يقدّمها، سواء بالنسبة لتقدير القاضي أو لثقة بقيّة أطـــراف الدعوى[4].

---

(1) د/ عمر بن يونس، المرجع السابق، ص 1025.

(2) لمزيد من التفاصيل حول كيفية كتابة تقرير فنّي انظر: د/ برهامي أبوبكر عزمي، الشرعيّة الإجرائيّة للأدلة العلميّة، المرجع السابق، ص 396 وما بعدها.

(3) نصّت المادة (145) من قانون الإجراءات الجزائية الجزائري على " يحلف الخبير اليمين المقيّد لأول مرّة بالجدول الخاص بالمجلس القضائي يمينا أمام ذلك المجلس بالصيغة الآتي بيانها:

- أقسم بالله العظيم بأن أقوم بأداء مهمّتي كخبير على خير وجه وبكل إخلاص وأن أبدي رأيي بكل نزاهة واستقلال ــ

ولا يجدّد هذا القسم مادام الخبير مقيّدا في الجدول".

ويقابل هذا النص المادة(86) من قانون الإجراءات الجنائية المصري بنصّها "يجب على الخبراء أن يحلفوا أمام قاضي التحقيق يمينا على أن يبدوا رأيهم بالذمة وعليهم أن يقدموا تقريرهم كتابة". وانظر أيضا المادة (139) من قانون الإثبات المصري.

(4) د/ أحمد أبو القاسم، الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، المرجع السابق، ص28.

ولقد استقر الفقه والقضاء على أنّ أداء الخبير لليمين يوم تسليمه العمل يغنى عن أداءه اليمين عند مباشرة كل مأموريّة[1]، فإن كان الخبير من غير خبراء وزارة العدل المعينين بالقانون، أو كان اسمه غير مقيّد في الجدول، يجب في هذه الحالة استحلافه اليمين بأن يؤدي عمله بالصدق والأمانة(المادة 145/ 3 إجراءات جزائري).

2 ــ أداء الخبير لمأموريّته بنفسه وفي حدود ما نصّ عليه أمر أو حكم الندب[2] [3].

3 ــ خضوع الخبير للرقابة القضائية: يتعيّن على الخبير أن يتولّى مهمّته تحت رقابة القاضي الذي عيّنه وأن يبقى على اتصال دائم به لأجل إحاطته علما بتطورات الأعمال التي يقوم بها، فالخبير هو مساعد للقاضي ومعاون فنّي لا أكثر[4].

4ــ استجابة الخبير للطلبات التي قد يوجهها الأطراف أثناء تنفيذ عمليّة الخبرة، كتكليف الخبير بإجراء أبحاث معيّنة أو سماع أي شخص معيّن باسمه قد يكون قادرا على مدّهم بالمعلومات ذات الطابع الفنّي(المادة 152 إجراءات جزائري).

5 ــ تقديم التقرير الفنّي خلال المدّة المحدّدة بأمر أو حكم الندب، وإذا لم يودع تقريره في المهلة المحدّدة فإنّه يجوز للقاضي استبداله في الحين مع إلزامه بردّ جميع الأشياء و الأوراق والوثائق التي تكون قد عهد بها إليه في ظرف ثمان وأربعين ساعة (المادة 149إجراءات جزائري) وقد يتعرّض الخبير المقصّر إلى عقوبات تأديبيّة وحتّى جزائيّة [5].

3ـ **مدى حجيّة تقرير الخبير التقني:** بعد انتهاء الخبير من أبحاثه وفحوصاته، يتعيّن عليه أن يعدّ تقريرا يضمنه خلاصة ما توصّل إليه من نتائج بعد تطبيق الأسس والقواعد العلميّة الفنيّة على المسائل محل البحث[6]. ويخضع هذا التقرير شأنه شأن باقي وسائل الإثبات لتقدير القاضي، فالقانون لم يضف عليه أيّة قوة ثبوتيّة خاصّة، فهو لا يلزم القاضي، ولهذا الأخير مطلق

---

[1] د/ برهامي أبوبكر عزمي، المرجع السابق، ص 383 . نقض 21 4 1959 س 10 ص 479 طعن رقم 483 سنة 29 قضائية .

[2] إلا أنه باستطاعة الخبير الاستثارة في مسألة خارجيّة عن تخصّصه بفنيّن آخرين (المادة 149إجراءات جزائية جزائري) ويتعيّن على هؤلاء أن يحلفوا اليمين وفق الشروط المنصوص عليها في المادة (145) إجراءات جزائري.

[3] وفي ذلك نصّت محكمة النقض المصرية في إحدى القضايا المعروضة عليها ما يلي: " ..للمحكمة في حدود مالها من حق استظهار عناصر الجريمة ألاّ تتقيّد بما قد يعرض له الطبيب في تقريره من توفر نيّة القتل إذ إن مأموريّته قاصرة على حد إبداء رأيه الفنّي في وصف الإصابات وسبب القتل .." . طعن رقم 1354 لسنة 26 ق جلسة 14/ 1/ 1957، مجموعة الأحكام، ص 651.

[4] J- Michaud,le juge d' instruction et l'expert, R. S. C , 1975 ، p. 791.

[5] J- Bradel, la responsabilite' pénale de l'expert , R.S.C, 1986, p. 24.

[6] تنص المادة (153/ 1) من قانون الإجراءات الجزائية الجزائري : " يحرّر الخبراء لدى انتهاء أعمال الخبرة تقريرا يجب أن يشتمل على وصف ما قاموا به من أعمال ونتائجها، وعلى الخبراء أن يشهدوا بقيامهم شخصيّا بمباشرة هذه الأعمال التي عهد إليهم باتخاذها ويوقعوا على تقريراهم".

الحريّة في تقديره، فله أن يأخذ بنتائج الخبرة أو استبعادها كما يشاء، ولـه كـذلك أن يـأمر بإجراء خبرة تكميليّة[1].

أو القيام بخبرة مضادة أو مقابلة[2] لاسيما إذا تعارضت النتائج التـي توصّـل إليهـا الخبراء حول نفس المسألة أو تعارض تقرير الخبير مع شهادة أحد الشهود.

وتجدر الإشارة إلى أنّه وإن كان من المقرّر أن القاضي يملك سلطة تقديريّة بالنسبة لتقـدير الخبير الذي يرد إليه، إلاّ أنّ ذلك لا يمتدّ إلى المسائل الفنيّة فلا يجوز له تفنيدها إلاّ بأسـانيد فنيّة[3].

وفي رأينا، أنّه من الضرورة إعطاء قوّة إلزاميّة لتقرير الخبير التقني، وذلـك علـى أساس أنّ القاضي إذا رفض رأي الخبير فقد تعارض مع نفسه، إذ يعنـي ذلـك أنّـه أراد أن يفصل بنفسه في مسألة سبق أن اعترف في بادئ الأمر بأنّ الخبير يتمتّع فيها بمعرفة ودراية تفوق معرفته الشخصيّة.

وما يحدث عمليّا أنّ القاضي غالبا ما يسلم بما خلص إليه الخبير في تقريره، ويبنـي حكمه على أساسه، وهذا التصرّف منطقي من القاضي فلا شك في أنّ رأي الخبير ورد فـي موضوع فنّي لا اختصاص للقاضي به، وليس في شأن ثقافته أو خبرته القضائية أن تتيح لـه الفصل فيه، بالإضافة إلى ذلك هو الذي انتدب الخبير ووثق فيه ورأى أنّه مناسب لمهمّته[4].

ب ـ القواعد الفنيّة التي تحكم عمل الخبير التقني: بالإضافة إلى القواعد القانونيّة الـسابقة الـذكر والمتوفّرة في جميع التخصصات في مجال الخبرة، وجود قواعد خاصّة تنفرد بهـا الخبـرة

---

(1) يقصد بالخبرة التكميليّة: "الخبرة التي تأمر بها المحكمة عندما ترى نقصا واضحا في الخبرة المقدّمة إليها أو أنّ الخبير لم يجب عن جميع الأسئلة و النقاط الفنيّة المعيّن من أجلها أو أنها لم تستوف حقّها من البحث أو التحرّي، فتطلب المحكمة باستكمال النقص الملحوظ في تقرير الخبرة وتسند الخبرة التكميليّة إلى الخبير الذي أنجزها أو إلى خبير آخر". انظر: مولاي ملياني بغدادي، الخبرة القضائيّة في المواد المدنيّة، مطبعة حلب، الجزائر، 1992، ص 15 .

(2) كرّست المحكمة العليا الخبرة المضادة في قرارها الصادر بتاريخ 18/ 11/ 1998، تحت رقم 155373، بقولها:"إذا ثبت وجود تناقض بين خبرة وأخرى وتعذّر فضّ النزاع بين الطرفين، وجب الاستعانة بخبرة فاصلة وعدم الاقتصار على خبرة واحدة أو خبرتين تماشيّا مع متطلّبات العدل "

(3) نقض 29/ 5/ 1967، مجموعة أحكام النقض، السنة 18، ص 143. ونقض 27/11/ 1967، السنة 18، ق 251. وقضت في هذا المعنى بأنّ:" رأي الخبير الفنّي لا يصحّ تفنيده بشهادة الشهود، فإذا كانت المحكمة قد أطرحت رأي مدير مستشفى الأمراض العقليّة في الحالة العقليّة لشخص واستندت في القول بسلامة عقله إلى أقوال الشهود، فإنّها تكون قد أخلت بحقّ الدفاع وأسّست حكمها على أسباب لا تحمله" . نقض 12/11/ 1951، مجموعة القواعد القانونيّة، ج 1، ق 44، ص 541.

(4) د/ محمد مروان، وسائل الإثبات في المواد الجنائيّة في القانون الوضعي الجزائري، الجزء الثاني، ديوان المطبوعات الجامعيّة، الجزائر، 1998، ص 404.

التقنية وقبل الشروع في تبيان هذه القواعد يتعيّن علينا تحديد أهم المسائل التي يستعان فيها بالخبرة التقنيّة وهي كالتالي[1]:

1 ـ وصف تركيب الحاسوب وصناعته وطرازه ونوع نظام التشغيل وأهم الأنظمة الفرعيّة التي يستخدمها بالإضافة إلى الأجهزة الملحقة به وكلمات المرور أو السر ونظام التشفير.

2 ـ وصف طبيعة بيئة الحاسب أو الشبكة من حيث التنظيم ومدى تركيز أو توزيع عمل المعالجة الآلية ونمط وسائل الاتصالات وتردّد موجات البث وأمكنة اختزانها.

3 ـ وصف الوضع المحتمل لأدلة الإثبات والهيئة التي تكون عليها.

4 ـ التمكن من نقل أدلة الإثبات غير المرئيّة وتحويلها إلى أدلّة مقروءة، أو المحافظة على دعامتها بغير أن يلحقها تدمير أو إتلاف، مع إثبات أنّ المخرجات الورقيّة لهذه الأدلة تطابق ما هو مسجّل على دعائمها الممغنطة.

5 ـ بيان كيفية عزل النظام المعلوماتي دون إتلاف الأدلة أو تدميرها أو إلحاق ضرر بالأجهزة.

1 ـ **خطوات اشتقاق الدليل الالكتروني:** لمّا كانت عمليّة تجميع الأدلة الالكترونيّة، تعدّ من أهم وأصعب الأمور التي تواجه الخبير التقني، كان لزاما عليه أن يتّبع عدة خطوات من أجل اشتقاق هذا النوع المستحدث من الدليل، وتتمثل هذه الخطوات في المراحل التالية:

أولاً ـ خطوات ما قبل التشغيل والفحص:

أ ـ التأكد من مطابقة محتويات أحراز المضبوطات لما هو مدوّن عليها.

ب ـ التأكد من صلاحية وحدات النظام للتشغيل.

ج ـ تسجيل بيانات الوحدات المكوّنات المضبوطة، كالنوع والطراز، والرقم المسلسل ..

ثانيا ـ خطوات التشغيل والفحص:

أ ـ استكمال تسجيل باقي بيانات الوحدات من خلال قراءات الجهاز.

ب ـ عمل نسخة من كل وسائط التخزين المضبوطة وعلى رأسها القرص الصلب (Hard Disk)، لإجراء عمليّة الفحص المبدئي على هذه النسخة لحماية الأصل من أي فقد أو تلف أو تدمير، سواء من سوء الاستخدام أو لوجود فيروسات أو قنابل برامجيّة.

ج ـ تحديد أنواع وأسماء المجموعات البرامجيّة، برامج النظام(برامج التشغيل)، وبرامج التطبيقات، وبرامج الاتصالات..، وما إذا كان هناك برامج أخرى ذات دلالة بموضوع الجريمة، برامج إنشاء ومعالجة الصور في جرائم دعارة الأطفال مثلا.

---

[1] د/ هشام فريد رستم، الجوانب الإجرائيّة للجرائم المعلوماتيّة، المرجع السابق، ص 142 و 143 .

د ـ إظهار الملفات المخبّاة، والنصوص المخفيّة داخل الصور.

هـ ـ استرجاع الملفات التي تمّ محوها من الأصل وذلك باستخدام أحد برامج استعادة البيانات، وكذلك بالنسبة للملفات المعطلة أو التالفة، مثل برنامج Recover4all) Professional Easy Recover). وبعد ذلك تخزّن هذه الملفات أو البيانات، ويعمل لها نسخ طبق الأصل أخرى من الأسطوانة أو القرص المحتوي لها لفحصها عن طريق تطبيق الخطوات سالفة الذكر .

و ـ يتم إعداد قائمة يجرّد فيها الخبير كل الأدلة الالكترونيّة التي تمّ الحصول عليها في الديسك الخاص به مع إجراء مراجعة لكل صورة محتفظ بها في الديسك في كمبيوتر آخر للتأكد من سلامة القائمة[1].

ي ـ تحويل الدليل الالكتروني إلى هيئة ماديّة وذلك عن طريق طباعة الملفات، أو تصوير محتواها إذا كانت صور أو نصوص، أو وضعها في أيّ وعاء آخر حسب نوع البيانات والمعلومات المكوّنة للدليل.

ثالثا: تحديد مدى الترابط بين الدليل المادي والدليل الالكتروني:

في هذه المرحلة يتمّ فحص كل من الدليل المادي المضبوط، و الدليل الالكتروني في شكله المادي، ومن تمّ الربط بينهما ممّا يكسب الدليل الموثوقيّة واليقينيّة، اللتان تؤديان إلى قبوله لدى جهة التحقيق والحكم.

رابعا: مرحلة تدوين النتائج وإعداد التقرير:

حيث يتمّ إعداد تقرير بجميع خطوات وإجراءات البحث، ويرفق به في الغالب الملاحق الإيضاحيّة المصوّرة أو المسجّلة وغيرها لاعتمادها ثمّ تسلّم إلى جهة الحكم و القضاء.

2 ـ **أدوات جمع الدليل الالكتروني:** يقوم الخبير التقني في سبيل تحري الحقيقة الاستعانة بكل ما يمكنه من التوصل إليها، وهو في إطار القيام بعمله قد يستخدم العديد من الأدوات والبرمجيات التي تمكّنه الحصول على الدليل الالكتروني، وتعتبر هذه الأدوات في نفس الوقت أساسية لأجهزة البحث والتحري والتحقيق بصفة عامة، ومن بين هذه البرمجيات المستخدمة في جمع الأدلة الالكترونيّة كالتالي:

---

[1] د/ ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، المرجع السابق، ص 2265.

أ ـ برنامج أذن التفتيش (Computer Scorch Warrant Program)

وهو برنامج قاعدة بيانات، يسمح بإدخال كل المعلومات الهامة المطلوبة لترقيم الأدلة وتسجيل البيانات منها ويمكن لهذا البرنامج أن يصدر إيصالات باستلام الأدلة والبحث في قوائم الأدلة المضبوطة لتحديد مكان دليل معين أو تحديد ظروف ضبط هذا الدليل.

ب ـ قرص بدء تشغيل الكمبيوتر (Bootable Diskette)[1]:

وهو قرص يُمكن المحقق من تشغيل الكمبيوتر، إذا كان نظام التشغيل فيه محمياً بكلمة مرور ويجب أن يكون القرص مزوداً ببرنامج مضاعفة المساحة (Double space) فربما كان المتهم قد استخدم هذا البرنامج لمضاعفة مساحة القرص الصلب.

ج ـ برنامج معالجة الملفات مثل (X tree Pro Gold):

وهو برنامج يُمكن المحقق من العثور على الملفات في أي مكان على الشبكة أو على القرص الصلب، ويستخدم لتقييم محتويات القرص الصلب الخاص بالمتهم أو الأقراص المرنة المضبوطة أو يستخدم لقراءة البرامج في صورتها الأصلية، كما يُمكن من البحث عن كلمات معينة أو عن أسماء ملفات أو غيرها.

د ـ برنامج النسخ مثل (Lap Link)

وهو برنامج يمكن تشغيله من قرص مرن ويسمح بنسخ البيانات من الكمبيوتر الخاص بالمتهم ونقلها إلى قرص آخر سواء على التوازي (Parallel Port) أو على التوالي (Serial Port) وهو برنامج مفيد للحصول على نسخة من المعلومات قبل أي محاولة لتدميرها من جانب المتهم.

هـ ـ برامج كشف الديسك مثل (View disk،AMA Disk)

يمكن من خلال هذا البرنامج الحصول على محتويات القرص المرن، مهما كانت أساليب تهيئة القرص، وهذا البرنامج له نسختان، نسخة عادية خاصة بالأفراد ونسخة خاصة بالشرطة[2].

---

[1] راجع المهندس/ حسن طاهر داود "جرائم نظم المعلومات" الإصدار رقم 244 لأكاديمية نايف العربية للعلوم الأمنية – الرياض – السعودية ، 2000، ص 228 وما بعدها.

[2] راجع الدكتور/ ممدوح عبد الحميد، زبيدة محمد جاسم وعبد الله عبد العزيز، المرجع السابق، ص 2243 وما بعدها.

و- برامج اتصالات مثل (LANtastic)

وهو يستطيع ربط جهاز حاسب الخبير أو المحقق بجهاز حاسب المتهم لنقل ما بـــه من معلومات وحفظها في جهاز نسخ المعلومات ثم إلى القرص الصلب.

هذه هي أهم الطرق العامة لجمع الأدلة الرقمية، والتي يجب أن يقوم بها خبراء فـــي هـــذا المجال نظراً لعلمية ودقة هذه الأدلة.

وبعد دراستنا لأهم القواعد القانونية والفنية للخبرة التقنية' ينبغي علينا التنويه بأن الدولة مهما كانت قوية تكنولوجيا إلاّ أنّها لا تقدر وحدها على مواجهة الإجرام الالكتروني، بل لابد من تعاون دولي في مجال الخبرة التقنية، وذلك من خلال عقد المؤتمرات وحضور الندوات، والاستفادة من تجارب الدول الأخرى، كما ينبغي تخصيص ميزانيّة معينة لتأهيل الخبراء إلى مستوى معين حتى يصبحوا قادرين على التعامل مع هذا النوع المستحدث من الأدلة الالكترونية.

المطلب الثاني

الإجراءات الحديثة لجمع الدليل الالكتروني

ذكرنا سلفا من خلال المطلب الأول مجموعة من الإجراءات التقليدية للحصول على الدليل الالكتروني، وتبيّن من خلالها مدى الصعوبات التي تحيط بها في ذلك، وهذا ما يسهّل للكثير من المجرمين الإفلات من العقاب، لدى فمن الضروري أن تواكب التشريعات المختلفة هذا التطوّر الملحوظ وذلك من خلال خلق قواعد قانونية إجرائيّة غير تقليدية لهذا الإجرام غير التقليدي، لذلك يكون من الضروري الاعتماد على تقنية تكنولوجية المعلومات في جمع الدليل الالكتروني، وذلك إمّا من أجل تيسير التجميع التقليدي للدليل الالكتروني كالتفتيش والضبط، ومن تمّ تضل هذه الإجراءات فعالة إزاء التغيير في بيئة تكنولوجيا المعلومات، أو تبني إجراءات حديثة مستقلة قائمة بذاتها.

وبما أنّ البيانات في بيئة التكنولوجيا ليست دائما ساكنة، بحيث يمكن أن تكون متحركة عبر شبكة من الشبكات، لذلك ينبغي أن يتلاءم الإجراء وطبيعة البيانات محل هذا الإجراء. فبالنسبة للبيانات الساكنة (الفرع الأول) يتمّ اللجوء إلى التحفظ العاجل على هذه البيانات، والأمر بتقديم بيانات معلوماتية متعلقة بالمشترك. أما بالنسبة للبيانات المتحركة (الفرع الثاني) يتم اللجوء إلى اعتراض الاتصالات الالكترونية الخاصة.

الفرع الأول
الإجراءات المتعلقة بالبيانات الساكنة

إنّ الإجراءات الخاصة بالبيانات الساكنة أو المتحركة كلها مستقاة من اتفاقية بودابست المنعقدة في (23 نوفمبر 2001 م) [1]، وهي أولى المعاهدات الدولية التي تكافح تلك الجرائم الالكترونيّة وهذه الاتفاقية تمت تحت إشراف المجلس الأوربي، ووقع عليها ثلاثون دولة بما في ذلك الدول الأربعة من غير الأعضاء في المجلس الأوربي المشاركة في إعداد هذه الاتفاقية وهي كندا واليابان وجنوب إفريقيا والولايات المتحدة الأمريكية حيث صادقت عليها هذه الأخيرة في(22 ديسمبر 2006) ودخلت بالفعل حيز النفاذ في الأول من يناير 2007 . وهي مفتوحة لانضمام دول أخرى حتى يمكن أن تساهم في ضبط و تنظيم مجتمع المعلومات و الاتصالات بشكل أفضل ،وتتكون هذه الاتفاقية من ثمانية وأربعين (48) مادة تم توزيعها على أربعة أبواب، يعالج الباب الأول منها: استخدام المصطلحات، ويتناول الباب الثاني الإجراءات الواجب اتخاذها على المستوى القومي ، ويضم هذا الباب ثلاث أقسام : أولها للقانون العقابي المادي أو الموضوعي، وثانيها للقانون الإجرائي، وثالثها للاختصاص القضائي.

ونحن سنتناول الجانب الإجرائي منها باعتباره موضوع بحثنا لاسيما في مجال الإجراءات المستحدثة والتي تقررها الاتفاقيّة.

وتتمثل الإجراءات المتعلقة بالبيات الساكنة في التحفظ العاجل على هذه البيانات(أولا)، ثمّ الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك(ثانيا).

أولا- التحفظ المعجل على البيانات المخزنة: نصّت اتفاقية بودابست في المادة(16) منها على ضرورة كل طرف السماح لسلطاته المختصة أن تأمر أو تفرض بطريقة أخرى مزود الخدمة

---

[1] للاطلاع على النص الكامل لاتفاقية بودابست ، يرجى مراجعة الموقع الخاص بالمجلس الأوربي :
http://www.convention .coe.int/treaty/EN/treaties/htm1/185.htm

وقد جاء في ديباجة اتفاقية المجلس الأوربي حول الإجرام السيبيري بيانا لمخاطر انتشار شبكة المعلومات على ما يلي:

ـــ " اقتناعا من الدول أعضاء مجلس الاتحاد الأوربي بضرورة منح الأولوية للسعي من اجل تنفيذ سياسة جنائية مشتركة تهدف إلى حماية المجتمع من إخطار جرائم الانترنت، وهي التي تشمل أمورا من بينها تبني التشريع المناسب ودعم التعاون الدولي.

ـــ و إدراكا لعمق التغيرات التي أحدثها التحول إلى الرقمية وارتباط شبكات الكمبيوتر مع بعضها البعض مع استمرار عولمتها .

ـــ و انشغالا بمخاطر احتمال استخدام شبكات الكمبيوتر و المعلومات الالكترونية أيضا في ارتكاب جرائم جنائية ...." .

التحفظ العاجل على البيانات المعلوماتية المخزنة بما في ذلك البيانات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتي، وذلك عندما تكون هناك أسباب تدعو للاعتقاد بأنّ هذه البيانات على وجه الخصوص معرّضة للفقد أو التغير، وذلك خلال مدة 90 يوم كحد أقصى، وهذه المدّة قابلة للتمديد.

نلاحظ مما سبق ذكره في المادة أعلاه أنّ إجراء حفظ البيانات يعد لبعض الدول خاصة العربيّة(كالجزائر ومصر) سلطة قانونية جديدة، فهو أداة تحقيق مستحدثة في إطار مكافحة الجرائم الالكترونية، فهو يتلاءم وطبيعة هذه البيئة من حيث قابلية البيانات فيها للمحو والفقد بسرعة، وقد نصّ المشرع الأمريكي على هذا الإجراء في القسم (f) (18 U. S .C2703) من قانون خصوصية الاتصالات الالكترونية الأمريكي (ECPA)[1]، وسنتناول فيما يلي تحديد مفهوم هذا الإجراء ، وقبل ذلك نوضح المقصود بمزودي الخدمات باعتباره الحائز لهذه البيانات ومدى التزامه بالتعاون مع سلطات التحري والتحقيق .

أ ـ المقصود بمزودي الخدمات: مزود الخدمات هو من يقدم خدمته إلى الجمهور بوجه عام في مجال الاتصالات الالكترونية التي لا تقتصر في أدائها على طائفة معينة من المتعاملين معه بمقتضى عقد من العقود[2]. ويَعرف قانون حماية الحياة الخاصة في مجال الاتصالات الالكترونية في الولايات المتحدة الأمريكية (ECPA) نوعين من مزودي الخدمات: **النوع الأول** مزودو خدمة الاتصالات الالكترونية، **والنوع الثاني** هم مزودو خدمة معالجة المعلومات عن بعد. ويقصد بالنوع الأول: كل من يقدم خدمة إلى مستخدمي الشبكة والتي تتمثل في تسهيل إرسال واستقبال الاتصالات السلكية والالكترونية [3].

---

[1] Agent may direct providers to preserve existing record pending the issuance of compulsory legal process. Such requests have no prospective effect however. بمعنى" يمكن لرجال الضبط القضائي توجيه مزودي الخدمات للتحفظ على سجلات موجودة في انتظار اتخاذ إجراء قانوني إجباري، ومع ذلك فإن مثل هذه الطلبات ليس لها تأثيرا مستقبلا ".

[2] د/ شيماء عبد الغني، المرجع السابق، ص 209. وقد عرّفت المذكرة التفسيريّة لاتفاقيّة بودابست مزود الخدمات في المادة الأولى(1) فقرة(ج) بأنّه" كل من يقوم بخدمات الاتصال أو خدمات معالجة البيانات أو خدمات تخزين البيانات، وقد يكون جهة عامة أو جهة خاصة، وقد يقدّم خدماته للجمهور أو لمجموعة من المستخدمين الذين يشكلون مجموعة مغلقة (كشركة مثلا). انظر: د/ هلالي عبد الله أحمد، المرجع السابق، ص 47ـ 48.

[3] د/ عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت في القانون الأمريكي، المرجع السابق، ص281.

أمّا النوع الثاني: فيعرّف حسب ما جاء في القسم (2) (c) (18 U S.C 2703) من قانون خصوصية الاتصالات الالكترونية الأمريكي) بأنه " كل من يقدم للجمهور خدمة معالجة البيانات عن بعد بوسيلة من وسائل الاتصالات الالكترونية ".

وبناء عليه إذا أرسل شخص لشخص آخر رسالة عن طريق البريد الالكتروني فإنّها تمرّ بالضرورة بمزود خدمة الاتصالات الالكترونية، وقبل أن يتلقاها المرسل إليه، تضلّ مخزنة لدى مزود الخدمات، فإذا تلقاها المرسل إليه فإن موقف هذا الأخير يتراوح بين أمرين: إما أن يقوم بمسح تلك الرسالة أو أن يقوم بتخزينها، في هذا الفرض الأخير تعتبر الرسالة مخزنة لدى مزود خدمة الاتصالات الالكترونية.

ب ـ التزام مزودو الخدمات بمدة معيّنة للتخلص من البيانات: تضع بعض التشريعات المقارنة كالقانون الفرنسي التزاما على مزودي الخدمات بإزالة البيانات التي يتم تخزينها تلقائيا وتتعلق بالاتصالات الالكترونيّة بين مستعملي شبكة الانترنت والتي تتعلق بهويّة المتصلين وساعة الاتصال[1] [2]، بل إن القانون الفرنسي المسمى **بالأمن اليومي** والصادر في (15 نوفمبر سنة 2001) قد أورد عقوبات في حالة عدم قيام مزود الخدمات بمسح تلك البيانات، وذلك احتراما لحرمة الحياة الخاصة (المادة:L 39-3) من قانون الأمن اليومي.

إلاّ أنّ هذا القانون السابق قد أورد نوعين من الاستثناءات على هذا الالتزام :

ــ يتعلق الأول بمتطلبات المحاسبة الماليّة بين مزودي الخدمات والمشتركين في خدماتهم، حيث يقدم مزودو الخدمات لبعض هؤلاء المشتركين بعض الخدمات مدفوعة الأجر.

ــ أمّا الاستثناء الثاني يتعلق باعتبارات التعاون من الجهات القضائيّة التي تبرر الاحتفاظ بتلك البيانات لمدة لا تزيد على سنة [3]. وهذا الاستثناء يؤكده التوجيه الأوربي رقم (58 لسنة

---

[1] Art. L. 32-3-1 alinéa 1 du code des postes et télécommunications dispose que:
" Les opérateurs de télécommunications‹ et notamment ceux mentionnés à l'article 43-7 de la loi n°86-1067 du 30 septembre 1986 précitée‹ sont tenus d'effacer ou de rendre anonyme toute donnée relative à une communication dès que celle-ci est achevée‹ sous réserve des dispositions des II‹ III et IV".

[2] ينبغي التنبيه أن المشرع الفرنسي مدّ التزام مزودي الخدمات في الحفاظ على البيانات المتعلقة بشخصية المتراسلين عبر شبكة الانترنت، وأسماء المواقع التي رجعوا إليها، ليشمل **محتوى المراسلة نفسها** والتي كان يحظر قانون الأمن اليومي الاحتفاظ بها، ليصبح ذلك جائزا بمقتضى قانون الأمن الداخلي لسنة 2003، وبالتالي يصبح القانون الفرنسي يتوافق مع قانون خصوصيّة الاتصالات الالكتروني الأمريكي(ECPA).

[3] Art. L. 32-3-1 alinéa 2 du code des postes et télécommunications dispose que:" Pour les besoins de la recherche‹ de la constatation et de la poursuite des infractions pénales‹ et dans le seul but de permettre‹ en tant que de besoin‹ la mise disposition de l'autorité judiciaire d'informations‹ il peut être différé pour une durée maximale d'un an aux opérations tendant à effacer ou à rendre anonymes certaines catégories de données techniques".

2002)، حيث قرر أنّه من حق الدول الأعضاء اتخاذ التدابير اللازمة لحماية الأمن العام والدفاع القومي وأمن الدولة والتحقيق في الجرائم بما يتضمّنه ذلك من وضع استثناءات على الحق في الخصوصيّة، ومن بين هذه الاستثناءات ضرورة التحفظ المعجل على البيانات المعلوماتية المخزنة حفاظا عليها من التلف والتغيير.

وتجدر الإشارة في هذا المقام أنّه ترد بعض الاستثناءات على التزام مزودي الخدمات بالتعاون مع سلطات التحقيق، حيث يستبعد القانون الفرنسي البيانات التي تحوزها جهات معيّنة من القاعدة السابقة والتي تفرض واجب التعاون مع رجال العدالة بوجه عام، وذلك مثل ما نصّت عليه الفقرة الثانية من المادة(31)من القانون رقم (17 لسنة 78 الصادر في 6 يناير 1978)، الخاص بالمعلوماتية والحريات في فرنسا، فتنص الفقرة الثانيّة من المادة31 من هذا القانون على عدم جواز مراقبة المعلومات التي تجمعها الكنائس أو أي تجمعات دينيّة أو فلسفيّة أو سياسيّة أو نقابيّة والتي تتعلق بأعضائها والمتراسلين معها.

كما تستثنى أيضا من القاعدة السابقة الذكر أنواع معينة من المعلومات نصت عليها المادة (18) من قانون الأمن الداخلي الذي عدّل قانون الإجراءات الجنائية الفرنسي حيث أن أدخل المادة (60 -1) وهي الخاصة بالمعلومات التي يغطيها سر المهنة، فتنص المادة السابقة على أنّه "باستثناء المعلومات التي تعتبر من أسرار المهنة التي أوردها القانون، والمتواجدة في الأنظمة المعلوماتيّة أو أيّ أجهزة للمعالجة الآليّة ..".

ج ـ مفهوم التحفظ المعجل على البيانات المخزنة[1]: يقصد به "توجيه السلطة المختصة لمزودي الخدمات الأمر بالتحفظ على بيانات معلوماتية مخزنة في حوزته أو تحت سيطرته، في انتظار اتخاذ إجراءات قانونيّة أخرى كالتفتيش أو الأمر بتقديم بيانات معلوماتية". وحتى تستوضح الصورة لنا عن هذا الإجراء نعطي مثالا عليه: "قد يعلم رجال الضبط القضائي بوجود صور داعرة للأطفال في اليوم الأول فيقومون باتخاذ إجراءات الحصول على إذن تفتيش في اليوم التالي، وفي اليوم الثالث يحصلون على الإذن ثمّ يصل علمهم أنّ المزود قام بشطب السجلات كالمعتاد في اليوم الثالث المذكور".

---

[1] هناك فرق بين التحفظ على البيانات"la conservation des données" والاحتفاظ أو أرشفة البيانات "l'archivage des données" ويقصد بالأول حفظ بيانات سبق وجودها في شكل مخزن، وحمايتها من كل شيء يمكن أن يؤدي إلى إتلافها أو تجريدها من صفتها أو حالتها الراهنة. أما الثاني فيقصد به تجميع البيانات والاحتفاظ بها في المستقبل بدون ضمان سلامتها وسريتها، فهو عملية تخزين لا غير.

ويتضح من المثال السابق أنّ التحفظ العاجل إجراء أولي أو تمهيدي الهدف منه هو محاولة الاحتفاظ بالبيانات قبل فقدانها، وقد حدّدت المذكرة التفسيرية لاتفاقية بودابست الأسباب التي تدعو إلى اتخاذ مثل هذا الإجراء وذلك للمبررات التالية :

1. قابلية البيانات المعلوماتية للتلاشي، حيث تكون محلا للمحو أو التغيير سواء كان ذلك بدافع إجرامي – بهدف طمس معالم الجريمة وأي عنصر إثباتي لشخصية المجرم –، أو بدافع غير إجرامي وذلك في إطار الحذف الروتيني للبيانات التي لم تعد الحاجة إليها.
2. غالبا ما يتمّ ارتكاب الجرائم الالكترونيّة عن طريق نقل الاتصالات عبر نظم الحاسوب، حيث يمكن أن تتضمن هذه الاتصالات محتويات غير مشروعة، مثل مواد إباحية للأطفال أو فيروسات الحاسوب، أو الدليل على ارتكاب جرائم أخرى مثل الاتجار بالمخدرات فتحديد مصدر إرسال هذه الاتصالات يمكن أن يساعد في تحديد هوية مرتكبي الجريمة .
3. تأمين الدليل الالكتروني من الضياع، حيث يتمّ نسخ الاتصالات ذات المحتوى غير المشروع أو دليل على نشاط جنائي من قبل مزودي الخدمات، مثل المراسلة الالكترونية التي تمّ إرسالها أو استقبالها، ومن تمّ يمكن الكشف عن دليل جنائي للجرائم المرتكبة.

وتجدر الإشارة أنّ البيانات المعلوماتية المشمولة بالأمر تتضمن بينها بيانات المرور المتعلقة باتصالات سابقة، وذلك من أجل تحديد خط سير الاتصال بمعنى مصدر أو مكان وصول هذه الاتصالات والتي تعدّ من الأمور الجوهريّة للتعرف على هويّة الأشخاص الذين قاموا بتوزيع مواد إباحيّة طفولية مثلا. وقد عرّفت **المادة الأولى فقرة "د"** من اتفاقية بودابست هذا النوع من البيانات (البيانات المتعلقة بالمرور) " بأنها صنف من بيانات الحاسوب التي تشكل محلا لنظام قانوني محدّد، حيث يتمّ توالد هذه البيانات من الحواسيب عبر تسلسل حركة الاتصالات لتحديد مسلك الاتصالات من مصدرها إلى الجهة المقصودة، وبذلك فهي تشمل طائفة من البيانات تتمثل في: مصدر الاتصال ووجهته المقصودة، خط السير ووقت أو زمن الاتصال وفقا لتوقيت غرينتش، حجم الاتصال ومدته ونوع الخدمة المؤذاة(مثل نقل الملفات أو بريد الكتروني أو مراسلات فوريّة). وفي الغالب ما يحوز مقدم الخدمة بمفرده بيانات المرور ما يكفي للتحديد بدقة مصدر أو نهاية الاتصال، بل إن كل واحد منهم (يحوز) يكون لديه بعض أجزاء اللغز، ويتعيّن أن توضع هذه الأجزاء تحت الاختبار بقصد تحديد مصدرها والجهة المرسلة إليها.

ثانيا- الأمر بتقديم بيانات معلوماتيّة متعلّقة بالمشترك: الأصل أنّ البيانات الشخصيّة المتعلقة بمستخدمي الشبكة تدخل في إطار الحق في الخصوصيّة التي تحميه الاتفاقيّة الأوربية لحقوق الإنسان والحريات الأساسية (بتاريخ 4 نوفمبر 1950)، فلا يجوز لمزود الخدمات أو غيره أن يقوم بإفشاء ما لديهم من معلومات إلى الغير. إلاّ أنّ بعض التشريعات المقارنة تسمح لرجال الضبط القضائي أن يأمروا الأشخاص بتسليم ما تحت أيديهم من موضوعات والتي يطلب تقديمها كدليل، ومن بينها البيانات المتعلقة بالمشترك التي يحوزها مزودو الخدمات، وهو ما يلزمه القانون الفرنسي رقم(719 لسنة 2000)المعدل للقانون رقم(1067 لسنة 1986) الخاص بحريّة الاتصالات، حيث تنص المادة(43ـ9) منه على" أنّه يتعيّن على مزودي خدمات الدخول والمسكّنين المحافظة على بيانات مستعملي خدماتهم وذلك تمهيدا لطلب السلطات منهم تلك البيانات التي قد تفيد كدليل في جريمة معيّة وقعت بالفعل.

أمّا بالنسبة للقانون الأمريكي المعروف بقانون خصوصية الاتصالات الالكترونيّة (ECPA)، فقد أجاز لرجال الضبط القضائي في إطار ما يقومون به من جمع الاستدلالات الاطلاع على البيانات الموجودة في حوزة مزودي الخدمات والتي تخص مستخدمي شبكة الانترنت، وذلك من خلال توجيه تكليف إلى مزود الخدمات بتقديم تلك المعلومات، وتتمثل هذه الأخيرة في ثلاث طوائف هي:

أولا ـ المعلومات الشخصية الخاصة بالمشترك مثل اسمه ورقم تلفونه وعنوانه.

ثانيا – المعلومات الشخصية الخاصة بالمتعامل مع المشترك(أي كل من يتّصل به أو يدخل معه في صفقة).

ثالثا – المعلومات المتعلقة بمحتوى البيانات (مضمون المحادثات ــ مضمون الملفات) .

والملاحظ أنّ التشريعات ذات الأصل اللاتيني مثل(القانون الفرنسي، الجزائري والمصري) تختلف عن القانون الأمريكي، حيث لا تجيز تلك التشريعات أن يصدر رجل الضبط القضائي مثل هذا الأمر، وإنّما تجيزه لسلطة التحقيق، حيث تنص المادة (99 إجراءات جنائية مصري) على أنّه " لقاضي التحقيق أن يأمر الحائز لشيء يرى ضبطه أو الاطلاع عليه بتقديمه، ويسري حكم المادة (274) على من يخالف ذلك الأمر ..."، ولا تختلف سلطة النيابة العامة في ذلك عن سلطة قاضي التحقيق. كما أن للمحكمة أن تصدر مثل هذا الأمر وفقا للقانون المصري، حيث تنص المادة(291) إجراءات مصري "للمحكمة أن تأمر ولو من تلقاء نفسها، أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة".

أمّا بالنسبة لاتفاقية بودابست فقد نصت في المادة (18) منها على " أنّه يجوز للدول الأطراف في تلك الاتفاقية تمكين السلطات المختصة من إلزام مقدمي الخدمات تقديم البيانات

المتعلقة بالمشترك، سواء كانت في حيازته المادية أو تحت سيطرته حيث تكون هذه البيانات مخزنة بعيدا عن الحيازة المادية لمزود الخدمة، ولكن يمكن السيطرة عليها، ومثال ذلك أن تكون البيانات مخزّنة في وحدة تخزين عن بعد ويتم تقديمها عن طريق شركة أخرى. ويشترط في هذه البيانات أن تكون مخزّنة ، حيث يستثنى منها أية معلومات متعلقة بحركة ومحتوى البيانات ذات العلاقة باتصالات مستقبلية، لأنّها تكون محل دراسة الفرع الثاني من هذا المطلب والخاص بالإجراءات المتعلقة بالبيانات المتحركة، هذا من جهة .

ومن جهة أخرى، ينبغي تحديد السلطة المختصة بإصدار أمر تقديم البيانات، حيث يسمح لرجال السلطة العامة بإصدار مثل هذا الأمر إذا تعلق الأمر بيانات المشترك المعلنة للجمهور، في حين أنّ دولا أخرى تشترط أن يكون هذا الأمر صادرا فقط من السلطات القضائيّة، عند الحصول على نوعية معيّنة من البيانات المتعلقة بالحق في الخصوصيّة مثل رقم بطاقة ائتمان أو حساب بنكي للمشترك.

وقد حدّدت الاتفاقية المقصود بتلك البيانات بقولها أنها تتعلّق:

- بنوع خدمة الاتصال التي اشترك فيها الشخص والوسائل الفنية لتحقيقها.
- العنوان البريدي أو الجغرافي ورقم تلفون المشترك.
- رقم دخول المشترك للحصول على تلك الخدمة والفواتير التي ترسل إليه، وأي معلومات تتعلق بطريقة الدفع (مثل رقم بطاقة الائتمان أو حسابه البنكي)، أو أي معلومات أخرى تتعلق بأداء الخدمة أو بالاتفاق بين هذا المشترك ومزود الخدمة.

الفرع الثاني

الإجراءات المتعلقة بالبيانات المتحركة (اعتراض الاتصالات الالكترونيّة)

تتجسد الإجراءات المتعلق بالبيانات المتحركة في **اعتراض**[1] **الاتصالات الالكترونيّة الخاصة**[2] [3]، ويقصد بهذا الإجراء مراقبة الاتصالات الكترونية أثناء بثها أي(في الزمن الفعلي لنقلها بين أطراف الاتصال)، وليس الحصول على اتصالات الكترونية مخزنة، ذلك أنّ لكل من النوعين قواعد خاصة بها ذلك من حيث صرامة ضمانات الحصول عليها في الأولى وخفتها في الثانيّة. ويثار في هذا الخصوص مشكلة تحديد طبيعة البريد الالكتروني غير المفتوح والمنتظر في صندوق خطابات مقدم خدمات الانترنت حتى يقوم المرسل إليه بإدخالها في نظامه المعلوماتي (أي استردادها)، فهل يجب اعتبارها بيانات معلوماتية مخزنة وبالتالي تطبق عليها الإجراءات المتعلقة بالبيانات الساكنة أم أنّها بيانات في مرحلة النقل والتحويل، وبالتالي تطبق عليها الإجراءات المتعلقة بالبيانات المتحركة والمتمثلة في اعتراض الاتصالات الالكترونية. ومن ثمّ لا يتمّ الحصول عليها إلاّ عن طريق سلطة الاعتراض.

---

[1] أغفل المشرع المصري في قانون الإجراءات الجنائيّة تعريف **الاعتراض** أو كما يسميه البعض (المراقبة)، واكتفى بوضع تنظيم لهذه العمليّة في المادتين (95 و 206) من القانون المذكور، ونفس الأمر بالنسبة للمشرع الجزائري. في حين عرّف الباب الثالث من القانون الفدرالي الأمريكي الاعتراض والتي يرمز إليها بكلمة"interception"، أنّه " **الاكتساب السمعي أو أي اكتساب لمحتويات أي اتصال سلكي أو الكتروني أو شفوي باستخدام أي جهاز الكتروني، أو ميكانيكي أو أي جهاز آخر**". وقد قضي بأنّ المقصود بكلمة الاكتساب "Acquisition" أن يتمّ الالتقاط أثناء الاتصال نفسه ومن تمّ تسجيله. لمزيد من التفصيل انظر: د/ شيماء عبد الغني، المرجع السابق، ص 305 وما بعدها.

[2] عرّف قانون الاتصالات الالكترونيّة الأمريكي لسنة 1986 **الاتصالات الالكترونيّة** بأنها:" كل انتقال بشكل كلي أو جزئي للإشارات أو الصور أو الأصوات أو المعطيات أو المعلومات أيّا كان نوعها، عن طريق الكابل أو الراديو أو النظام الكهرومغناطيسي أو التصوير الكهربائي أو الصور المرئيّة. في حين عرّف قانون البريد والاتصالات الالكترونيّة الفرنسي Code des postes et des communication eléctroniques, Décret n° 80-567, Journal Officiel du 23 juillet 1980) الاتصالات الالكترونيّة (بأنها:" كل انتقال أو إرسال أو استقبال لإشارات أو علامات أو كتابة أو صور أو أصوات عن طريق النظام الكهرومغناطيسي.

[3] يرى البعض (مثل د/ شيماء عبد الغني) أنّ المحادثات الفوريّة والمعروفة بنظام الشات(Chat)، بالإضافة إلى المحادثات المعروفة بالدردشة ــ أين يمكن التحدث مع أكثر من شخص في الوقت ذاته ــ ، لا تنطبق عليها الحماية الجنائيّة التي تتمتع بها المحادثات الشفويّة التي تتم في مكان خاص، لان شبكة الانترنت لا تعتبر مكانا خاصا ومن ثمّ يجوز مراقبة هذه الأحاديث العامة دون قيد أو شرط، وهذا الرأي ينطبق على الفريق الذي يعتد بطبيعة المكان لإضفاء صفة الخصوصيّة على الحديث بخلاف الرأي الذي يعتد بموضوع المحادثة، حيث يكون الحديث في نظرهم خاصا متى كان موضوعه يمس الحياة الخاصة للمتحدث، بغض النظر عن مكان حدوثه (سواء عاما أو خاصا).

حسم المشرع الأمريكي هذا الأمر، واعتبر الاتصالات الالكترونية المخزنة من قبيل البيانات الساكنة وبالتالي تطبق عليها كل الإجراءات التي تتناسب هذا النوع من البيانات من تفتيش والأمر بالتحفظ العاجل وتقديم هذه البيانات، بدليل أنه قام بتعديل القسم (2703) من قانون خصوصية الاتصالات الالكترونيّة (ECPA)، ليشمل حماية الاتصالات الالكترونية المخزنة من بريد الكتروني والرسائل الصوتية غير المفتوحة والمخزنة لدى مزود الخدمة. وقد تم تأكيد هذه القاعدة في العديد من التطبيقات القضائية مثل قضيّة (United States v. Smith)[1]، حيث قرّر القضاء بأنه لا يمكن مراقبة الاتصالات السلكية وهي في حالة التخزين الالكتروني [2].

وقد ميّزت اتفاقية بودابست بين نوعين من البيانات المعلوماتيّة محلّ الاعتراض، بين **البيانات المتعلقة بالمرور والبيانات المتعلقة بمحتوى الاتصال**، وبالنسبة للنوع الأول فإنّ المادة الأولى(1) من الاتفاقيّة قد عرّفتها بأنّها" كل البيانات التي تعالج الاتصالات التي تمرّ عن طريق نظام معلوماتي، والتي يتمّ إنتاجها بواسطة هذا النظام المعلوماتي بوصفه عنصرا في سلسلة الاتصال، مع تعيين المعلومات التاليّة: أصل الاتصال، مقصد الاتصال أو الجهة المقصودة بالاتصال، خط السير، ساعة وتاريخ، حجم وفترة الاتصال، أو نوع الخدمة.

أمّا بالنسبة للنوع الثاني: **البيانات المتعلقة بمحتوى الاتصال** فإنّه لم يأت تعريف لها في الاتفاقيّة لكنّها تشير إلى المحتوى الإخباري للاتصال، بمعنى مضمون الاتصال أو الرسالة أو المعلومات المنقولة عن طريق الاتصال، فيما عدا البيانات المتعلقة بالمرور.

ويلاحظ ممّا سبق ذكره أنّ هناك نوعا من التقارب بين هذين النوعين من البيانات، من حيث المعنى إلاّ أنهما مختلفان تماما من حيث درجة المساس بالحق في الخصوصيّة، حيث يكون ذلك أكثر أهميّة بالنسبة لمراقبة محتوى الاتصال أو المراسلة، ومن ثمّ تفرض ضمانات أكبر عند تجميع محتوى البيانات في الزمن الفعلي عن حركة البيانات سواء من حيث الجرائم التي من أجلها يتمّ توظيف هذا الإجراء، أو من حيث السلطة المختصة بإصدار أمر المراقبة.

وقد أكّدت اتفاقية بودابست هذا التمييز حيث أدرجت كل إجراء على حدة تحت عنوان خاص، فخصّت تجميع حركة البيانات بعنوان" **التجميع في الزمن الفعلي لبيانات المرور**"[3]

---

[1] United States v. Smith، 155 F. 3d 1051، 1058-59 (9thCir. 1998).

مشار إليه عند د/ عمر محمد بن يونس، المرجع السابق، ص 369 وما بعدها.

[2] لمزيد من التفاصيل حول هذه القضيّة، أنظر: د/ عمر محمد بن يونس، المرجع السابق، ص 369 وما بعدها.

[3] Collecte en temps réels des données relatives au trafique.

(المادة 20)، أما تجميع محتوى البيانات فجاء تحت عنوان " **اعتراض محتوى البيانات**"[1] (المادة 21).

وعلى العكس من ذلك تضع بعض الدول مفهوما موحدا لكل من تجمع حركة البيانات ومراقبة محتوى البيانات ومن ثمّ يسري عليهما نفس الضمانات الخاصة عند اتخاذ احد الإجراءين، دون أخذ في الاعتبار إلى الحساسيّة التي تحيط بموضوع مراقبة محتوى البيانات. ويرجع السبب في ذلك إلى عدم وجود تمييز في القانون الذي لا يوجد فيه اختلافات حول المصلحة في الخصوصيّة أو لتشابه إجراءات التجميع التقني ومن هذه الدول فرنسا.

وتجدر الإشارة إلى أنّ حق الإنسان في الخصوصيّة ليس حق مطلق، بل مقيد بالمصلحة العامة وقد تتعارض خصوصية الإنسان مع مصلحة المجتمع في كشف الحقيقة في شأن الجريمة ومعاقبة الجناة، مما يستلزم وجود توازن دقيق بين الحق في الخصوصية وحق المجتمع في العقاب، وحتى نحقق هذا التوازن ينبغي إحاطة هذه المراقبة بضمانات تكفل استعماله في نطاق الهدف الذي شرع من أجله. لذلك سنتناول في التالي النقاط التالية: مدى تمتع الاتصالات بصفة عامة والالكترونيّة بصفة خاصة بالحماية الجنائيّة(أولا) ثمّ الحالات التي يكون فيها الاعتراض مشروعا سواء كان ذلك من دون سبق الحصول على إذن أو بناء على إذن(ثانيا).

أوّلا: حرمة الاتصالات الالكترونيّة الخاصة:

ممّا لاشك فيه أنّ مراقبة الأحاديث الخاصة تمسّ بحق الإنسان في الخصوصيّة وما يتفرّع عنه من سريّة الأحاديث الخاصة، وهو حق لصيق الصلة بالإنسان ــ بل هو على حد قول أحد الفقهاء ــ الإنسان نفسه[2]. وهذا الحق أصبح مهدّدا بدرجة كبيرة، نتيجة للتطور التكنولوجي الذي أدى إلى إفراز أجهزة للمراقبة ذات تقنيّة، تلتقط أحاديث الإنسان دون أن يشعر، ولم تقتصر هذه الأجهزة على التنصت(interception) على الاتصالات السلكيّة واللاسلكيّة فحسب[3]، بل امتدت بقدرتها الفائقة إلى التقاط الاتصالات التي تتمّ بطريق

---

(1) Interception de donnée relatives au contenue.

(2) Alain F.Westin، Privacy and Freedom، New York، 1967، p.37.

مشار إليه عن: د/ ياسر الأمير فاروق محمد، مراقبة الأحاديث الخاصة في الإجراءات الجنائيّة، دراسة مقارنة، رسالة دكتورا، كلية الحقوق، جامعة القاهرة، 2008، ص 11.

(3) Guerrier (C), les écoutes téléphoniques, N.R.S. Droit, Paris p. 1.

وانظر كذلك: د/ فتحي عبد النبي الوحيدي، الأثر السلبي للتطور التكنولوجي على الحريّات الشخصيّة، مجلة روح القوانين، العدد 13، يونيو 1998، ص 2. وانظر أيضا: د/ عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنّفات الفنيّة، ودور الشرطة والقانون، دراسة مقارنة، بدون تاريخ ودار النشر، ص 264 وما بعدها.

الانترنت[1]، ممّا أفقد الإنسان حريّته وخصوصيّته، وهدّد على نحو خطير كرامته وإنسانيته، الأمر الذي حِد ببعض الفقهاء إلى القول بأنّ أجهزة المراقبة السمعيّة تعدّ نكسة (retombée) للتقدم المذهل للتقنيات الحديثة.

ونتيجة لذلك حرصت أغلب التشريعات على توفير قدر كبير من الحماية الجنائيّة على سريّة الاتصالات الخاصة للأفراد، حيث عاقب المشرع الجزائري لأوّل مرة اعتراض الاتصالات السلكيّة واللاسلكية دون إذن بذلك، بموجب القانون رقم(06ـــ 23 المؤرخ في 20 ديسمبر سنة 2006) المعدّل لقانون العقوبات الجزائري، حيث تنص المادة (303 مكرر) من قانون العقوبات على أنّه: " يعاقب بالحبس من ستة(6) أشهر إلى ثلاث (3) سنوات وبغرامة من 50،000دج إلى 300،000دج كل من تعمّد المساس بحرمة الحياة الخاصة للأشخاص، بأي تقنيّة كانت وذلك :

1. بالتقاط أو تسجيل أو نقل مكالمات أو أحاديث خاصة أو سريّة، بغير إذن صاحبها أو رضاه .
2. بالتقاط أو تسجيل أو نقل صورة لشخص في مكان خاص، بغير إذن صاحبها أو رضاه."

ويعاقب على الشروع في هذه الجرائم بنفس عقوبات الجريمة التامة.

ولم تقتصر الحماية عند تجريم الأفعال الخاصة بالاعتراض، بل شملتها أيضا إلى عقاب كل من احتفظ أو وضع أو سمح بأيّة وسيلة كانت التسجيلات المتحصل عليها بأحد الأفعال المنصوص عليها في المادة (303 مكرر) من هذا القانون.

أمّا بالنسبة للمشرع المصري فقد عاقب بالحبس مدّة لا تقل عن سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرّح بها قانون أو بغير رضا المجني عليه:

أ- استرق السمع أو سجّل أو نقل عن طريق جهاز من الأجهزة أيّا كان نوعه محادثات جرت في مكان خاص أو عن طريق التلفون.

ب- التقط أو نقل بجهاز من الأجهزة أيّا كان نوعه صورة شخص في مكان خاص.

وباستقرائنا لنص المادتين(303 مكرر) من قانون العقوبات الجزائري والمادة(309 مكرر) عقوبات مصري، نلاحظ أنّهما يخصان المحادثات الخاصة أو التي تتم في مكان

---

[1] د/ أحمد حسام طه تمام، الحماية الجنائيّة لتكنولوجيا الاتصالات، دراسة مقارنة، دار النهضة العربيّة، 2002، ص35.

خاص[1]، وأيضا التي تتمّ عن طريق تلفوني، دون المحادثات التي تتمّ عن طريق الكمبيوتر، والتي تتخذ شكل البريد الالكتروني أو شكل المحادثة الفوريّة.

ونتيجة لذلك قامت العديد من التشريعات بإدخال نصوص خاصة تسري على الاتصالات الالكترونيّة، أي تلك التي تتم بطريق الكمبيوتر، بالإضافة إلى الاتصالات السلكيّة واللاسلكيّة. منها ما تضمّنه القانون الجنائي الفدرالي الأمريكي(Title 18، Part 1، Chapter 119، Sec.2511) على عقاب من قام باعتراض المراسلات الالكترونيّة، مساويا في ذلك بينها وبين الاتصالات السلكيّة، حيث نص على عقاب كل من اعترض أو حاول إعتراض أو ساعد غيره على أن يعترض أو يحاول اعتراض أي اتصال سلكي أو شفوي أو **الكتروني**.

وعلى ذلك نرى أنّه يتعيّن على المشرع الجزائري والمصري أن يتدخلا لسن قوانين خاصة، لتنظيم الوضع القانوني للمحادثات الالكترونيّة ولا يتركها لاجتهاد المحاكم لمعرفة ما إذا كان الوضع القانوني لهذه المحادثات تسري عليه القواعد الخاصة بالاتصالات السلكيّة. خاصة وأنّ هذا النوع من المحادثات وان كان يتمّ عن طريق خط تلفوني، فما هو إلا وسيلة للدخول على الشبكة فقط .

ثانيا: الاعتراض المشروع للاتصالات الالكترونية الخاصة:

ذكرنا سلفا أنّ الأصل في اعتراض الاتصالات الالكترونية الخاصة هو الحظر، إلاّ بإذن قضائي مسبق، ولكن هناك حالات يكون فيه الاعتراض مشروعا دون صدور هذا الإذن.

أ ـ سلطة مزود الخدمات في مراقبة النظام دون إذن: ويكون ذلك إمّا في إطار المراقبة المعتادة لمزود الخدمة لمتابعة عمل الشبكة، أو تكون بناء على شكوى المشترك، وسنحاول دراسة ذلك بالتفصيل في التالي:

1ـ المراقبة المعتادة لمزود الخدمة لعمل الشبكة: نصّت بعض التشريعات المقارنة صراحة ــ كالقانون الأمريكي ــ في (المادة (18 U .S.C. § 2511 (2)(a)(I)) على حق مزودي الخدمات في مراقبة الاتصالات الالكترونيّة الخاصة بالمشتركين في خدماتهم، وذلك في إطار العمل اليومي لشبكاتهم، من أجل حماية أنظمتهم من إساءة الاستعمال أو من الإضرار بها (عن طريق استعمال الفيروسات) أو الاستيلاء عليها بالسرقة مثلا.

---

[1] لمزيد من التفصيل حول المعايير التي تعتد بها التشريعات الجنائية لتحديد مفهوم الحديث الخاص محل الاعتراض سواء بالمعيار الموضوعي (مدى تعلق محتوى الحديث بالسرية) أو بمعيار شكلي(معيار طبيعة المكان). انظر: د/ طارق سرور، حق المجني عليه في تسجيل المحادثات التليفونيّة الماسة بشخصه، دار النهضة العربيّة، الطبعة الثانيّة، 2004، ص 18 وما بعدها. وانظر كذلك: د/ ياسر الأمير فاروق، المرجع السابق، ص 521 وما بعدها. وانظر أيضا: د/ محمود أحمد طه، التعدي على حق الإنسان في سريّة اتصالاته الشخصيّة بين التجريم والمشروعية، مجلة روح القوانين، العدد 9 ، يناير 1993، ص 80 وما بعدها.

ومن التطبيقات القضائية على هذا النوع من المراقبة ما قضي به من أنّه يجوز لمزودي الخدمات أن يقوموا بتلك المراقبة لمكافحة الغش والسرقة الواقعة على الخدمات التي يقدمونها، من ذلك أن يقوم أحد الأشخاص بتقليد خط لتلفون محمول للحصول على الخدمة دون دفع الاشتراك، الأمر الذي يقتضي أن يتابع مزود تلك الخدمة هذا الخط المقلد لتحديد مكانه ومعرفة الفاعل لذلك[1].

ومن الجدير بالذكر أنّ المشرّع الأمريكي لم يطلق سلطة مزودي الخدمات في ممارسة تلك الرقابة بل اشترط عدة شروط ينبغي توافرها لصحة هذه الرقابة وتتمثل فيما يلي:

1 ــ أن يكون مزود الخدمات مجنيا عليه في جريمة.

2 ــ أن يقوم بالمراقبة وبالتبليغ عما يعلمه من جرائم إلى الجهات القضائيّة، حماية لحقوقه وليس قياما بدور المساعد للمباحث في التحريّات التي يقومون بها.

3 ــ ألاّ يطلب رجل الشرطة من مزود الخدمات القيام بتلك المراقبة عونا له، أي أنّ المبادرة بالتبليغ يجب أن تأتي من جانب مزود الخدمات.

4 ــ ألا يشارك رجل الشرطة أو يشرف على مزود الخدمات في قيامه بأعمال المراقبة[2].

2ـ **المراقبة بناء على شكوى المشترك:** اختلفت التشريعات المقارنة حول مدى إمكانية السماح للسلطات بمراقبة الاتصالات الالكترونية بناء على الطلب الصادر من صاحب الجهاز محل الاعتداء بوضع جهازه تحت المراقبة من قبل رجال الضبط القضائي بذلك (ويقاس هذا الاستثناء على مزود الخدمات)، وكان الأمر يدور بين موقفين : أحدهما مؤيد والثاني معارض لهذه المراقبة.

بالنسبة للموقف المعارض يجسده رأي في كندا، ويعتبر فيه أن مزود الخدمات متماثل في عمله مع رجال السلطة العامة، وبالتالي فإنّه ليس من حقه القيام بتلك الرقابة وتلك التسجيلات بدون إذن، فإذا قام بذلك فإنّه يخالف حكم المادة (24 فقرة2) من ميثاق الحقوق والحريّات الكندي.

أمّا بالنسبة للموقف المؤيد لهذا النوع من المراقبة، فيجسّده القانون الأمريكي، حيث يسمح القسم (18 U .S.C.Sec. 2511 (2) (I لضحايا الهجوم على الحاسوب بتفويض السلطات لمراقبة الاتصالات السلكية والالكترونيّة التي يتمّ بثها إلى أو من الجهاز محل الاعتداء.

---

[1] United States v. Pervaz، 118 F.3ed. 1،5 (1st Cir)

مشار إليه عند د/ شيماء عبد الغني، المرجع السابق، 222.

[2] د/ عمر محمد بن يونس، المرجع السابق، ص 386 وما بعدها.

ويلزم لتوافر هذا الاستثناء اجتماع أربعة شروط وهي:

الشرط الأول : أن يسمح المالك ـــ أو صاحب الحق ـــ لرجال الضبط بوضع الجهاز الخاص به تحت المراقبة.

الشرط الثاني: أن يتمّ ذلك في إطار تحقيق جنائي قائم.

الشرط الثالث : أن تتوافر دلائل كافية على أن تسجيل الاتصالات القادمة من الجهاز الصادر منه الاعتداء يفيد في كشف الحقيقة.

الشرط الرابع: أن يقتصر رجال الضبط على اعتراض الاتصالات الصادرة من وإلى الأجهزة محل التحقيق.

وفي تحديد مفهوم "المعتدى على النظام"، يستبعد القانون الأمريكي من هذا المفهوم كل من تربطه علاقة تعاقدية مع مزود الخدمة والذي يتجاوز الحدود التي تسمح بها تلك العلاقة (المادة (21) 18 U .S.C. § 2511)، ومثال ذلك مستخدمو شركة معيّنة لا يعتبرون في عداد المعتدين على النظام إذا استغلوا أجهزة الشركة في أغراض أو في أوقات بالمخالفة لنظام الشركة.

ب ـ اعتراض الاتصالات الالكترونية بناء على إذن: ممّا لاشك فيه أنّ الحماية التي يكفلها المشرّع للاتصالات العادية لا يقتصر نطاقها على هذا النوع من الاتصالات فحسب، بل تمتدّ هذه الحماية إلى الاتصالات الالكترونية عبر الانترنت من باب أولى بحسبان أنّ الغاية من وراء هذه الحماية هي حماية الحياة الخاصة للإنسان بحماية مستودع أسراره الشخصيّة، وهذه الأسرار تكون أكثر انتهاكا إذا ما استخدمت الوسائل الالكترونيّة في الوصول إليها، ومن ثمّ فإنّها تكون في حاجة إلى حماية أكثر من تلك الحماية التي تحتاجها الاتصالات العادية. وإذا اقتضت ضرورة التحقيق اعتراض هذه الاتصالات وتسجيلها، فسنتبع حينها نفس الضمانات المقررة للمحادثات التلفونيّة، مع مراعاة خصوصيّة هذه الاتصالات الحديثة. وتتمثل أهم الضمانات القانونيّة فيما يلي:

- **السلطة المختصة بإصدار إذن الاعتراض:** السلطة القضائيّة هي المختصة عموما بإصدار هذا الإذن ويعدّ ذلك ضمانة لازمة لمشروعيّة الاعتراض على الاتصالات السلكية واللاسلكية في القانونين المصري والفرنسي[1]، حيث أنّها ضمانة ضد افتئات أجهزة الدولة على حرمة

---

[1] Article 100 de CPP francais dispose que: "En matière criminelle et en matière correctionnelle, si la peine encourue est égale ou supérieure à deux ans d'emprisonnement, **le juge d'instruction** peut، lorsque les nécessités de l'information l'exigent, prescrire l'interception، l'enregistrement et la transcription de correspondances émises par la voie des télécommunications .... "

الحياة الخاصة، وقد نص الدستور المصري على هذه الضمانة في المادة 45 منه وجاءت المادتان(95 و206) من قانون الإجراءات الجنائية لتؤكد ذلك، ويتّضح من نص هاتين المادتين أنّ المشرع استلزم صدور الإذن بالاعتراض من قاضي التحقيق المختص أو من القاضي الجزئي، وحرمان النيابة العامة من إصدار هذا الإذن،وذلك للحدّ من سلطة هذه الأخيرة منعا لأيّ تعسف، ولكن في حالة ما إذا كانت النيابة العامة تتولى التحقيق بنفسها وتبيّن لها ضرورة اعتراض المحادثات التلفونيّة للمتهم كان عليها طبقا لنص المادة (206 إجراءات مصري) أن تحصل على إذن من القاضي الجزئي بمراقبة المحادثات التلفونيّة[1]، وهو ما أكّدت عليه محكمة النقض في حكم لها حيث قرّرت" أنّ المشرع أباح لسلطة التحقيق وحدها ــ وهي قاضي التحقيق وسلطة الاتهام في أحوال التصدي للتحقيق أو إجراء تحقيقات تكميليّة وللنيابة العامة في التحقيق الذي تجريه بعد استئذان القاضي الجزئي ..". ولا يشترط أن يقوم قاضي التحقيق أو النيابة العامة في حالة صدور إذن من القاضي الجزئي بتنفيذ أمر الاعتراض، بل لهما أن يعهدا ذلك لمأمور الضبط القضائي[2] إلاّ أنّ المشرّع الجزائري خالف، ذلك وأجاز لوكيل الجمهوريّة المختص أن يأذن باعتراض المراسلات التّي تتمّ عن طريق وسائل الاتصال السلكية واللاسلكيّة، وذلك في المادة (65 مكرر 5) من قانون الإجراءات الجزائيّة الجزائري.

وتجدر الإشارة إلى أنّ الطبيعة الخاصة التي يتمتع بها الدليل الالكتروني من حيث سرعة فقده وزواله، تفرض علينا أن نخفف من حدّة شرط ضرورة استئذان النيابة العامة القاضي الجزئي حتى تتمكّن من مباشرة الاعتراض في الحالة التي تتولى التحقيق بنفسها بصدد جريمة من الجرائم الالكترونيّة وتبيّن لها ضرورة اعتراض وتسجيل اتصالات الكترونية عبر الانترنت. وذلك كسبا للوقت للتحفظ على الدليل وضبطه.

- **فائدة الإعتراض في إظهار الحقيقة**: تقرّر التشريعات المعاصرة أنّ" ضابط فائدة المراقبة في ظهور الحقيقة" يعتبر السند الشرعي المبرر للاعتراض، ذلك بسبب أنّ هذا الإجراء يتضمن اعتداءا جسيما على حرمة الحياة الخاصة وسريّة الاتصالات، فيباح استثناء وفي حدود

---

[1] إلاّ أنّ هناك حالات خاصة يعقد فيها الاختصاص للنيابة العامة بصفة استثنائيّة في مباشرة إجراء الاعتراض دون حاجة للحصول على إذن من القاضي الجزئي، وذلك إذا تعلق الأمر بجناية تخص بنظرها محكمة أمن الدولة العليا وهي الجرائم المضرة بأمن الدولة زمن جهة الداخل وذلك بموجب نص المادة (2/7) من القانون رقم 105 لسنة 1980 والخاص بإنشاء محاكم أمن الدولة . انظر: د/ هبة أحمد علي حسانين، الحماية الجنائية لحرمة الحياة الخاصة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007، ص 396 .

[2] نقض 14 فبراير 1967، مجموعة أحكام النقض، س 18 رقم 42، ص 219. وأيضا نقض 25 أكتوبر 1972، س 24 رقم 219، ص 1053 .

ضيّقة وذلك للفائدة المنتظرة منه والتي تتعلق بإظهار الحقيقة بكشف غموض الجريمة وضبط الجناة [1]. ويترك لقاضي التحقيق أو للقاضي الجزئي تقدير مدى فائدة اعتراض المحادثات التلفونيّة في كشف الحقيقة ويخضع في هذا التقدير لرقابة قضاء الموضوع [2].

- **تسبيب الإذن القضائي الصادر باعتراض الاتصالات الالكترونيّة:** للقاضي أن يصدر الإذن بمراقبة الاتصالات الالكترونيّة بناء على ما يتكشّف له من خلال أعمال الاستدلال التي قام بها مأمور الضبط القضائي وتبيّن له من خلالها ضرورة إصدار الإذن بالموافقة لما لذلك من أهميّة في ظهور الحقيقة في جريمة ارتكبت خاصة الجريمة الالكترونيّة، وينتج هذا التسبيب بصفة عامة من مدى اقتناع القاضي بجديّة التحريّات التي اتخذها مـــأمور الضبط القضائي. والعلة التي من أجلها يتم تسبيب الإذن القضائي ترجع إلى أنّ هذا الإجراء يمس حريّات الأفراد فهو استثناء على القاعدة العامة والمتمثّلة في حرمة الحياة الخاصة للمواطنين وحقّهم في سريّة مراسلاتهم واتصالاتهم.
- **الجرائم التي يجوز فيها الاعتراض:** إذا كان المشرع الجزائري نصّ صراحة في المادة (65مكرر5)على نوع الجرائم التي يجوز فيها اعتراض المراسلات التي تتمّ عن طريق وسائل الاتصال السلكيّة واللاسلكية ومنها جرائم المساس بأنظمة الحاسب المعالجة الآليّة للمعطيات[3]، وذلك إدراكا منه على عدم كفاية الوسائل التقليدية لجمع الدليل الالكتروني نظرا لما تتمتّع به هذه الجريمة المستحدثة من خصوصيّة، إلا أنّ المشرّع المصري قد اعتمد على معيار جسامة العقوبة، حيث حدّد في المادتين (95 و206) الجرائم الجائز فيها "الاعتراض" وهي الجنايات والجنح المعاقب عليها لمدة لا تقل عن ثلاثة أشهر، هذا

---

[1] د/ محمد أبو العلاء عقيدة، مراقبة المحادثات التلفونيّة، دراسة مقارنة، دار الفكر العربي، 1994، ص 192.

[2] د/ محمود نجيب حسني، المرجع السابق، 1988، ص 668.

[3] تنص المادة (**65 مكرر 5**) من قانون الإجراءات الجزائيّة الجزائري على أنّه: " إذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي، في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنيّة، أو **الجرائم الماسة بأنظمة المعالجة الآليّة للمعطيات**، أو جرائم تبيض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد، يجوز لوكيل الجمهوريّة المختص، يأذن بما يأتي:

ـــ اعتراض المراسلات التي تتمّ عن طريق وسائل الاتصال السلكيّة واللاسلكيّة.

ـــ وضع الترتيبات التقنيّة، دون موافقة المعنيين، من أجل التقاط وتثبيت وبث وتسجيل الكلام المتفوه به بصفة خاصة أو سريّة من طرف شخص أو عدّة أشخاص في أماكن خاصة أو عموميّة أو التقاط صور لشخص أو عدّة أشخاص يتواجدون في مكان خاص".

ويشترط في الجريمة محل الاعتراض أن تكون قد وقعت فعلا، حتى يبنى على ذلك ضرورة صدور الإذن بالاعتراض[1].

- **مدّة الاعتراض:** حرصت معظم التشريعات المعاصرة على تحديد مدّة معيّنة للاعتراض منعا من التعسف وإساءة استعمال السلطة، غير أنّ هذه التشريعات لم تسر على وتيرة واحدة في شأن هذه المراقبة فمنها من حدّد المدة بأمد قصير كالمشرع المصري، حيث حددها بثلاثين (30) يوما قابلة للتجديد لمدة أو مدد أخرى مماثلة طبقا للتحديد الوارد في نص المادتين (95 و206) إجراءات مصري. أما البعض الآخر فقد أطال زمن المدّة إلى أربعة أشهر قابلة للتجديد، وذلك عند التشريعين الفرنسي(المادة 100 ـ2)[2] إجراءات فرنسي والجزائري (المادة 65 مكرر 7 الفقرة 2)[3] إجراءات جزائي جزائري.

وعلى ذلك، ترتب المراقبة الصحيحة التّي اتخذت في ظل احترام سائر الضوابط المقررة في القانون أثر يتعلّق بإمكانية الاعتداد بالأدلة الالكترونية (سواء كان بريد الكتروني أو محادثة فوريّة) الناجمة عنها في إثبات الجريمة الالكترونيّة ونسبتها إلى المتهم. أمّا المراقبة الباطلة فترتب أثر عكسي يتمثل في استبعاد الأدلة الناجمة عنها وعدم جواز قبولها في إثبات إدانة المتّهم، فضلا عن تحقق المسؤوليّة الجنائيّة عن جريمة الاعتراض غير المشروع (المادة 309 مكرر عقوبات مصري) إذا توافرت الشروط التي يتطلّبها القانون لقيام هذه الجريمة[4].

---

(1) وهو ما أكدته محكمة النقض في قضائها بقولها:" الأصل في الإذن بالتفتيش أو بتسجيل المحادثات أنّه إجراء من إجراءات التحقيق لا يصح إصداره إلاّ لضبط جريمة ـ جناية أو جنحة ـ وقعت بالفعل وترجحت نسبتها إلى متهم معيّن وأنّ هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو حريته الشخصيّة. نقض 11 نوفمبر 1987، مجموعة أحكام النقض س 38 رقم 173، ص943. نقض 25 نوفمبر 1973، مجموعة أحكام النقض، س 24 رقم 219، ص 1053.

(2)Article 100-2 de CPP francais dispose que:" Cette décision est prise **pour une durée maximum de quatre mois**. Elle ne peut être renouvelée que dans les mêmes conditions de forme et de durée."

(3) تنص (المادة 65 مكرر فقرة 2) إجراءات جزائري على ما يلي:" يسلم الإذن مكتوبا **لمدّة أقصاها أربعة (4) أشهر** قابلة للتجديد حسب مقتضيات التحري أو التحقيق ضمن نفس الشروط الشكليّة والزمنيّة".

(4) د/ رؤوف عبيد، مبادئ الإجراءات في القانون المصري، دار الفكر العربي، 2006، ص 446.

الفصل الثاني

مدى اقتناع القاضي الجنائي بالدليل الالكتروني

إنّ مرحلة الحكم هي المرحلة الحاسمة في الدعوى الجنائيّة، ذلك أنّ غاية الدعوى هي الوصول إلى حكم حاسم لها، حائز قوّة إنهائها، ولهذا فإنّ الحكم يمثّل أهم إجراءات هذه الدعوى لأنّه يمثّل غايتها، وعمليّة تقدير الأدلة تشكل جوهر هذا الحكم، حيث لا يمكن الوصول إليه وإدراكه ما لم يمارس القاضي سلطته التقديريّة على الأدلة محل الوقائع، وفي مجال الجريمة الالكترونيّة يكون الدليل الالكتروني هو الأوفر، سيما إذا اعتبرنا الحكم هو الكلمة النهائيّة للقضاء، وهو غاية التنظيم القضائي برمّته، وسلامة هذا الحكم يتوقّف بدرجة كبيرة على سلامة التقدير للأدلة .

والدليل الالكتروني شأنه شأن باقي الأدلة الأخرى يخضع لنفس القواعد المقرّرة لباقي الأدلة، سواء كانت هذه القواعد تتعلق بسلطته في قبول الدليل الالكتروني، أو تتعلّق بسلطته في تقدير هذا النوع من الدليل، ذلك أنّ القاضي لا يقدّر إلاّ الدليل المقبول، ولا يكون مقبولا إلاّ بعد التيقن من مراعاة الدليل لقاعدة المشروعيّة والتي لا يمكن من دونها أن يترتّب الدليل الالكتروني أيّ آثار قانونيّة.

وبالنظر إلى الطبيعة الخاصة التي يتميّز بها الدليل الالكتروني، وما قد يصاحب الحصول عليه من خطوات معقّدة، فإنّ قبوله في الإثبات قد يثير العديد من المشكلات، حيث أنّ مستودع هذه الأدلة هو الوسائل الالكترونيّة، ولذا التلاعب فيها وتغيير الحقيقة أمر وارد، وهذا ما يجعلنا نتساءل: كيف نضمن مصداقيّة الدليل الالكتروني وأنّها بالفعل تعبّر عن الحقيقة التي تهدف إليها الدعوى الجنائيّة؟

وعلى ذلك، ستكون الإجابة على هذا الإشكال من خلال تعرضنا بالدراسة إلى:

ـ سلطة القاضي الجنائي في قبول الدليل الالكتروني وذلك في المبحث الأول، وفيه نتناول أساس قبول الدليل الالكتروني في الإثبات الجنائي(المطلب الأول)، ثمّ القيود التي ترد على حريّة القاضي الجنائي في قبول الدليل الالكتروني(المطلب الثاني).

ـ أمّا في المبحث الثاني سنخصصه لسلطة القاضي الجنائي في تقدير الدليل الالكتروني، وذلك من خلال مطلبين يتمثل الأول في حريّة القاضي الجنائي في الاقتناع بالدليل الالكتروني، أمّا المطلب الثاني سيكون مخصص الضوابط التي تحكم اقتناع القاضي بالدليل الالكتروني.

المبحث الأول
سلطة القاضي الجنائي في قبول الدليل الالكتروني

يعدّ قبول الدليل الخطوة الإجرائيّة الأوليّة التّي يمارسها القاضي تجاه الدليل الجنائي بصفة عامة والدليل الالكتروني بصفة خاصة، وذلك قبل البدء في تقديره، للتأكد من مدى صلاحيته، وملاءمته لتحقيق ما قدم من أجله، وقبول القاضي الجنائي الدليل الالكتروني في الإثبات لابدّ وأن يستند على أساس، وهذا الأخير يختلف من نظام إلى آخر سواء كان نظام لاتيني أو نظام أنجلو سكسوني.

ويهدف القاضي الجنائي في هذه المرحلة إلى التيقن من مدى مراعاة الدليل الجنائي أساسا لقاعدة المشروعيّة والتي لا يمكن بدونها أن يترتب على الدليل أي آثار قانونيّة، بل يثير إهمالها أو مخالفة ما يستلزمه من شروط آثار قانونية أخرى تكمن أساسا في بطلانه وبطلان كل ما ترتب عليه من إجراءات.

وعلى ضوء ما سبق بيانه سنتناول هذا المبحث في المطلبين التاليين:

المطلب الأوّل: أساس قبول الدليل الالكتروني في الإثبات الجنائي.

المطلب الثاني: القيود الواردة على حريّة القاضي الجنائي في قبول الدليل الالكتروني.

المطلب الأول
أساس قبول الدليل الالكتروني في الإثبات الجنائي

الواقع أنّ موقف القوانين المقارنة فيما يتعلّق بسلطة القاضي الجنائي في قبول الدليل الالكتروني تخضع إلى طبيعة نظام الإثبات السائد في الدولة ، وتنقسم هذه النظم إلى ثلاث فئات:

الفئة الأولى: تتبنى مبدأ حريّة الإثبات، ومنها سلطة القاضي في قبول جميع الأدلة، وهنا تكون جميع طرق الإثبات مقبولة، ما لم يستبعد المشرّع بعضها صراحة، كاستبعاد المراسلات بين المتهم ومحاميه مثلا، وينتمي إلى هذه الفئة القانون الفرنسي المادة(427) من قانون الإجراءات الجنائيّة والقانون الجزائري، المادة(212) من قانون الإجراءات الجنائيّة والقانون المصري (291) من قانون الإجراءات الجنائيّة .

الثانية: وتأخذ بنظام الأدلة القانونيّة، حيث تحدّد الأدلة التي يجوز للقاضي الجنائي قبولها، كالقانون الهولندي(المادة 339) من قانون الإجراءات الجنائيّة والقانون الألماني الذي يحدّد على سبيل الحصر وسائل الإثبات التي يتعيّن على القاضي قبولها[1]، وإن كان التطبيق العملي لهذين القانونين يتّجه نحو نظام حريّة الإثبات[2].

أما الفئة الثالثة والأخيرة: وهي القوانين الأنجلوسكسونيّة، حيث تقيّد من حريّة الإثبات في مرحلة الفصل في مسألة الإدانة أو البراءة، أمّا في مرحلة تحديد العقوبة فيسود مبدأ حريّة الإثبات[3].

وعلى ذلك، سنحاول من خلال الفروع المتقدّمة أن نبيّن موقف النظم القانونيّة من الدليل الالكتروني كدليل إثبات، ومن البديهي أن يكون هذا الموقف مبنيّا على أساس قانوني لقبول هذا النوع المستحدث من الأدلة، وسنتناول دراسة هذا الأساس في الفرع الأول، أمّا في الفرع الثاني، سنخصّصه للقيود الواردة على حريّة القاضي الجنائي في قبول الدليل الالكتروني.

---

(1) وهذه الوسائل هي: سماع أو سؤال المتهم (der Angeklagte)، وشهادة الشهود(die Zeugen)، وتقارير الخبراء (die Schachverstandigen)، الانتقال للمعاينة (der Augenschein)، والمستندات (die Urkunden).

(2) Pradel، la preuve en procédure pénale comparé، rapport général، in، revus international de droit pénal، 1992، p. 18.

(3) د/ أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائيّة المقارنة، الطبعة الثانيّة، دار النهضة العربيّة، القاهرة، 2006، هامش رقم 12، ص14.

الفرع الأول
في النظام اللاتيني

لم تفرد التشريعات المنتميّة إلى العائلة ذات الأصل اللاتيني مثل فرنسا، وغيرها من الدول المتأثرة بها كالجزائر ومصر، نصوصا خاصّة فيما يتعلق بقبول الدليل الالكتروني، وذلك على أساس أنّ هذه الدول تستند لمبدأ حريّة الإثبات في المسائل الجنائيّة، هذا المبدأ الذي يمثل لبّ نظام الإثبات الحر[1]، حيث أصبح هذا الأخير القانون العام في الإجراءات الجزائيّة في التشريعات اللاتينيّة، وبمقتضاه يحكم القاضي في الدعوى حسب العقيدة التي تكوّنت لديه بكامل حريّته، وتتمثل خصائص هذا النظام في عدم تحديد الأدلّة، بمعنى أنّ الخصوم لهم الحريّة في الالتجاء إلى أيّ دليل يمكنهم من إثبات ادعائهم، كما أنّ هذا النظام يخوّل القاضي سلطة تقييم الأدلة دون أن يفرض عليه قيدا أو شرطا، فالقاضي حرّ في أن يستعين بكل طرق الإثبات للبحث عن الحقيقة، وهو حرّ في وزن وتقدير كل دليل، وفي التنسيق بين الأدلة التي تتمثل في الحكم بالإدانة أو البراءة.

ونتيجة لذلك، فإنّه يحظر على المشرّع إضفاء قوّة معيّنة لأيّ دليل من شأنه أن يقيّد سلطة القاضي في تكوين قناعته، أو يسبغ على بعضها شكا أو عدم ثقة كي يستبعدها القاضي من تقديره الحر[2].

وانطلاقا مما سبق ذكره يتّضح لنا مبدئيّا أنّه يجوز للقاضي الجنائي الاستناد إلى الدليل الالكتروني لإثبات الفعل الجنائي في سائر الجرائم والجرائم الالكترونيّة على وجه الخصوص. وهو ما سوف نبيّنه بالتفصيل في التالي، من خلال دراسة أساس قبول هذا النوع المستحدث من الدليل في التشريعات ذات الأصل اللاتيني(أوّلا)، ثمّ نبينّ أهم النتائج المترتبة على الأخذ بهذا الأساس(ثانيا).

---

[1] يطلق عليه البعض نظام (الأدلة الأدبيّة)، أمّا البعض الآخر يطلق عليه نظام (الأدلة الاقناعيّة)، أو نظام (الاقتناع الشخصي أو الذاتي) (Système de l'intime conviction de juge)، وهناك من يسميه (حرية القاضي الجنائي في الاستسلام لنداء ضميره). لمزيد من التفصيل حول هذا النظام: انظر: د/ احمد فتحي سرور. أصول الإجراءات الجنائيّة، دار النهضة العربية، القاهرة، 1969، ص 343. وانظر كذلك: د/ مفيدة سويدان، نظريّة الاقتناع الذاتي للقاضي الجنائي، دكتوراه كليّة الحقوق، جامعة القاهرة، 1985، ص 109. د/ محمود نجيب حسني، المرجع السابق، ص 421.

[2] د/ فاضل زيدان محمّد، سلطة القاضي الجنائي في تقدير الأدلّة، دراسة مقارنة، رسالة دكتوراه، كليّة الحقوق، جامعة بغداد، 1992، ص 60.

أوّلا- مبدأ حريّة الإثبات الجنائي[1] كأساس لقبول الدليل الالكتروني:

تعتبر حريّة الإثبات في المسائل الجنائيّة من المبادئ المستقرّة في نظريّة الإثبات الجنائي، وذلك بخلاف المسائل المدنيّة حيث يحدّد القانون سلفا وسائل الإثبات وقواعد قبولها وقوّتها. ويقصد بهذا المبدأ: حريّة جميع الأطراف في اللجوء إلى كافة وسائل الإثبات للتدليل على صحّة ما يدّعونه، فسلطة الاتهام أن تلجأ إلى أيّة وسيلة لإثبات وقوع الجريمة على المتّهم، ويدفع المتّهم كذلك بكل الوسائل، ويستظهر القاضي الحقيقة بكلّ ذلك أو بغيره من طرق الإثبات[2]. إذن فجميع الأدلة متساوية لا تفاضل بينها إلا بمقدار ما تحدثه من أثر في نفس القاضي من ارتياح واطمئنان.

وقد استقرّ مبدأ حريّة الإثبات الجنائي منذ القديم على الرغم من أنّ " تقنين التحقيقات الجنائيّة الفرنسي" لم يكرّسه صراحة، وإنّما أشير إليه في بعض النصوص، خاصّة التعليمة المقرّرة للمحلفين لدى محكمة الجنايات[3].

وفي الوقت الحالي، فإنّ قانون الإجراءات الجنائيّة الفرنسي قد أقرّ مبدأ حريّة الإثبات الجنائي صراحة بمقتضى المادة(427) منه حيث تنص: " ما لم يرد نص مخالف، يجوز إثبات الجرائم بجميع طرق الإثبات، ويحكم القاضي بناء على اقتناعه الشخصي" [4]، وهذا النص وإن كان مخصّصا لمحاكم الجنح، إلاّ أنّ مبدأ حريّة الإثبات يطبق أمام جميع أنواع المحاكم الجنائيّة، إلاّ إذا نصّ القانون على خلاف ذلك[5]. وتأييدا لذلك تفرض محكمة النقض الفرنسيّة على محاكم الموضوع تطبيقا صارما لهذا المبدأ بحيث تفرض في النهاية حريّة كاملة للإثبات، فهي تشدّد في العديد من أحكامها على حريّة قضاة الموضوع في الاستعانة بأي دليل يكون

---

[1] يجب التمييز بين مبدأ حريّة الإثبات وحريّة القاضي في الاقتناع، وعدم الخلط بينهما، حيث يقصد بالأول الطريق الإثباتي المرسوم لكل أطراف الدعوى بما فيهم القاضي في اختيار وسائل الإثبات الملائمة للواقعة محل الإثبات، بينما يتعلّق الثاني بنطاق سلطة القاضي في تقدير وتقييم الدليل، بحيث يمثّل المبدأ الثاني الأساس الذي يسيطر على آخر مرحلة من مراحل تقدير الدليل الجنائي منذ نشأته حتى تحقيق غايته. انظر: د/ أحمد ضياء الدين محمد خليل، مشروعيّة الدليل في المواد الجنائيّة، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعيّة في مجال الإجراءات الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامع عين شمس، 1982 ص 248.

[2] د/ أحمد ضياء الدين محمد خليل، المرجع السابق، ص 240.

[3] المادة 342 من قانون التحقيقات الجنائيّة الفرنسي (Code d'instruction francais).

[4] Article 427 du (C.P.P) ، dispose que :" Hors les cas où la loi en dispose autrement، les infractions peuvent être établies par tout mode de preuve et le juge décide d'après son intime conviction".

[5] Merle et Vitu، op. cit، p. 165.

لازما لتكوين عقيدتهم، وأنّ الفقرة (2من المادة 427) تطبق على وسائل الدفاع[1]، بيد أنّ الدائرة الجنائيّة لمحكمة النقض الفرنسيّة ذهبت أكثر من ذلك في احترام مبدأ حريّة الإثبات، فهي ترى أنّه طالما لا يوجد نص قانوني يستبعد صراحة دليلا ما فلا يجوز للمحكمة عدم قبول هذا الدليل ولو كان ذلك الدليل غير مشروع بل لو كان عدم المشروعيّة ناتجة عن ارتكاب جريمة [2]،غير أنّها تشترط فحسب أن يكون هذا الدليل قد خضع للمناقشة الحضوريّة في الجلسة أي احترام حقوق الدفاع.

وكذلك أقرّ المشرع الجزائري مبدأ حريّة الإثبات الجنائي في المادة(212) من قانون الإجراءات الجزائيّة الجزائري حيث نصّت على أنّه: " يجوز إثبات الجرائم بأيّ طريق من طرق الإثبات ماعدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الشخصي"[3].

ونفس الشيء كرّسته المادة (291) من قانون الإجراءات الجنائيّة المصري حيث تنص على أنّ "للمحكمة أن تأمر ولو من تلقاء نفسها أثناء نظر الدعوى، بتقديم أيّ دليل تراه لازما لظهور الحقيقة"، وقد أكّدت محكمة النقض المصريّة [4] هذا المبدأ في العديد من أحكامها، بقولها" أنّ القانون ــ فيما عدا ما إستلزمه من وسائل خاصة للإثبات ــ فتح بابه أمام القاضي

---

[1] Cass ;Crim 12 avril 1995، B، n° 156. Cass ;Crim 15 juin 1993، B، n° 210، Cass ;Crim 25 septembre 1987، B، n° 316 .

[2] Cass ;Crim 15 juin 1993، B، n° 210. Cass ;Crim 6avril 1993، J.C.P، édition générale، n° 43، note Mme Rassat، p. 415.

[3] من الملاحظ أنّ المشرّع الجزائري أدرج نص المادة(212) من قانون الإجراءات الجزائيّة الجزائري ضمن الأحكام المشتركة والمتعلقة بطرق الإثبات أمام جهات، الحكم مما لا يدع أيّ شك في تطبيقها أمام كل الجهات القضائيّة الجزائيّة، في حين أنّ المشرع الفرنسي أورد نص المادة(427) قانون الإجراءات الفرنسيّة التي تقابل المادة(212) جزائري، ضمن أحكام الجنح، ممّا أثار جدلا فقهيّا حول تطبيقه أمام الجهات الأخرى إلاّ أنّ الكثير من الفقهاء يعتبرون أنّ حكم المادة(427) هو حكم عام، انظر في هذا الشأن:
G. Lauvasseur، La juridiction correctionnelle depuis l'application du code de procédure pénal، revus du science criminelle،1959، p. 577.

[4] تجدر الإشارة أنّ المحاكم المصريّة كانت قد استقرّت ــ قبل صدور قانون الإجراءات الجنائيّة الحالي (رقم 150 لسنة 1950) الصادر في سنة 1950 ــ على تطبيق مبدأ حريّة الإثبات، واستقرّت على أنّ للقاضي الجنائي حريّة الاستعانة بكافة وسائل الإثبات لتكوين اقتناعه حول حقيقة الوقائع المرفوعة عنها الدعوى. انظر على سبيل المثال: نقض 12 يونيه سنة 1939 ، مجموعة القواعد القانونيّة، الجزء الرابع، رقم 406، ص 575. نقض 11 يناير سنة 1943، مجموعة القواعد القانونيّة، الجزء السادس، رقم 68، ص 64.

الجنائي على مصراعيه يختار من كل طرقه ما يراه موصلا إلى الكشف عن الحقيقة ويزن قوّة الإثبات المستمدّة من كل عنصر[1].

وتكمن الأسباب الداعيّة لضرورة إعمال مبدأ حريّة الإثبات في نطاق نظريّة الإثبات الجنائي فيما يلي:

ـ أنّ حريّة الإثبات تعدّ نتيجة منطقيّة لمبدأ قضاء القاضي بمحض اقتناعه والتي تستتبع في نفس الوقت السماح للقاضي بالاستعانة بجميع وسائل الإثبات التي يقتنع ويطمئن إليها لتمكين القاضي من أداء رسالته في إرساء العدالة بين المتقاضيين.

ـ إنّ الإثبات في الدعوى الجنائيّة يرد على وقائع قانونيّة ـ ماديّة أو نفسيّة ـ يصعب بل يستحيل الحصول على دليل مسبق لها، وذلك بعكس الدعوى المدنيّة التي يرد الإثبات فيها على تصرفات وأعمال يسهل إعداد دليل مسبق بشأنها[2][3].

ـ إنّ محل الإثبات في الدعوى الجنائيّة يرد على وقائع قانونيّة تنتمي إلى الماضي، لذلك لابد للمحكمة أن تستعين بكل الوسائل الممكنة كي تعيد لها رواية ما حدث، خاصّة وأنّ الجناة يسعون إلى طمس آثار سلوكهم الإجرامي حتى يكون الدليل عليه مستحيلا.

ـ من المسلم به أنّ قرينة البراءة تلقي عبئ الإثبات كليّة على عاتق سلطة الاتهام ممّا جعلت مهمّة هذه الأخيرة جد صعبة[4]، لذلك كان من الضروري تسليح المجتمع ـ ممثلا في سلطة الاتهام ـ بمختلف الوسائل والصلاحيات التي تسمح بالقيام بواجبها.

ـ إنّ طبيعة المصلحة التي تحميها الدعوى الجنائيّة تختلف عن تلك التي تحميها الدعوى المدنيّة، فغالبا ما تتعلق الأولى بمصلحة المجتمع في أمنه واستقراره، أمّا المصلحة في الدعوى الثانية فهي خاصّة بأطرافها.

ـ مبدأ حريّة الإثبات يعدّ بمثابة إقرار ضمني من المشرع بعدم قدرة الأدلة التقليدية والتي لو تمّ حصرها كأدلة إثبات على مواجهة الجرائم المستحدثة ومنها الجريمة الالكترونيّة، بمعنى

---

(1) نقض 25 يناير 1965، مجموعة أحكام محكمة النقض، س 16 رقم 21، ص 87. نقض 20 يناير 1969، س 20 رقم 35، ص 164. وانظر كذلك: نقض 24 أبريل 1978، س 29 رقم 84 ، ص 442. وانظر أيضا: 25 نوفمبر 1984، س 29 رقم 185، ص 821.

(2) د/ محمد زكي أبو عامر، الإثبات في المواد الجنائيّة، الفنيّ للطباعة والنشر، الإسكندرية، بدون تاريخ النشر، ص 106. وانظر: د/ محمود نجيب حسني، المرجع السابق، ص 778وما بعدها. وانظر كذلك: د/ أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصّلة بطريق غير مشروعة، المرجع السابق، ص11.

(3) جيوفاني ليوني، مبدأ حرية الاقتناع والمشاكل المرتبطة به، ترجمة: د/ رمسيس بهنام، مجلة القانون والاقتصاد، العدد الرابع، السنة الرابعة والثلاثون، 1964، ص 926وما بعدها .

(4) د/ محمد زكي أبو عامر، المرجع السابق، ص 126.

فتح الباب لنوع من الأدلة العلميّة للاستفادة من الوسائل التي يكشف عنها العلم الحديث كبصمة الصوت، والبصمة الوراثيّة (D.N.A)، والدليل الالكتروني.

وعلى ذلك نلاحظ أنّه الدليل الالكتروني شأنه في ذلك شأن الأدلة الأخرى التي تمّ ذكرها على سبيل المثال في القانون، مقبول مبدئيا في الإثبات الجنائي بصفة عامة، والإثبات في مجال الجرائم الالكترونيّة بصفة خاصّة، إذا ما تمّ الاحترام فيه على ضابط المشروعيّة، ذلك لأنّ الحريّة هنا لا يقصد بها إمكان اللجوء إلى وسائل غير مقبولة قانونا، فحريّة الأطراف في مجال الإثبات يجب أن تمارس في إطار ما تفرضه عليه ضوابط المشروعيّة من قيود يستحيل مخالفتها، وإلاّ ترتب على ذلك عدم مشروعيّة ذلك الدليل، ومن ثمّ عدم قبوله بل بطلانه.

ثانيا- النتائج المترتبة على تطبيق مبدأ حريّة الإثبات الجنائي:

على ضوء ما تقدّم، فإنّ إعمال مبدأ حرية الإثبات يجعل القاضي الجنائي يتمتّع بدور إيجابي في توفير وقبول وتقدير الدليل الجنائي بما في ذلك الدليل الالكتروني.

وسوف نتناول من خلال التالي، دور القاضي الجنائي في توفير وقبول الدليل الالكتروني أمّا مسألة التقدير نتركها للمبحث الثاني والخاص بسلطة القاضي الجنائي في تقدير الدليل الالكتروني.

أ - الدور الايجابي للقاضي الجنائي في توفير الدليل الالكتروني: يؤدي القاضي الجنائي دورا هاما، بل لعله أكثر الأدوار أهميّة في الدعوى الجنائيّة، وبصفة خاصة في شأن عمليّة الإثبات، ولم يكن منح القاضي الجنائي هذا الدور سوى أحد مظاهر اعتناق المشرّع لمبدأ حريّة الإثبات، وحتّى يتّضح لنا هذا الدور المهم للقاضي الجنائي يتعيّن لنا أن نقوم بتحديد مفهوم هذا الدور بداية، ثم نعرض لأهم مظاهر الدور الايجابي للقاضي الجنائي.

1- مفهوم الدور الايجابي للقاضي الجنائي في توفير الدليل الالكتروني: يقصد به عدم التزام القاضي بما يقدّمه له أطراف الدعوى من أدلة، وإنّما له سلطة بل وواجب عليه أن يبادر من تلقاء نفسه إلى اتخاذ جميع الإجراءات لتحقيق الدعوى والكشف عن الحقيقة الفعليّة فيها[1]، ذلك أنّ الحقيقة لا تظهر من تلقاء نفسها، وإنّما في حاجة دوما إلى من يبحث وينقب عنها، وليس له أن يقنع بما يقدمه إليه أطراف الدعوى وإنّما عليه أن يبحث بنفسه عن الأدلة اللازمة

---

[1] د/ محمود محمد مصطفى، شرح قانون الإجراءات الجنائيّة، مطبعة دار النشر الثقافة، الطبعة الثانية القاهرة، 1953، ص 360.

لتكوين عقيدته على الوجه الصحيح لأنّه يسعى إلى اكتشاف الحقيقة الموضوعيّة أي الحقيقة في كل نطاقها [1].

وفي ذلك يختلف دور القاضي الجنائي عن دور القاضي المدني، فإذا كان عمل هذا الأخير مجرّد قبول الأدلة المقدمة من الخصوم في الدعوى، فليس له أن يبادر من تلقاء نفسه إلى البحث عن أيّ دليل أو تقديمه وأن يوجّه أحد الأطراف إلى تقديم دليل بعينه، بينما القاضي الجنائي لا يتخذ هذا الدور السلبي[2]، فمن حقّه بل من واجبه أن يتحرّى ويبحث عن الحقيقة بجميع الوسائل، سواء نصّ عليها القانون أم لم ينص عليها كالدليل الالكتروني مثلا، وقد أكّدت هذا المعنى المادة (212) من قانون الإجراءات الجزائيّة الجزائري والمادة (291) من قانون الإجراءات الجنائيّة المصري[3].

والنظام الإجرائي السائد في الدولة هو الذي يحدّد دور القاضي الجنائي، فحيث يكون النظام الاتهامي(Le procédure accusatoire)هو المتبني فمن الطبيعي أن يكون دور القاضي الجنائي في هذا الشأن سلبيا، لأنّ هذا النظام ينظر إلى الدعوى الجنائيّة على أنّها ملك لطرفين، الأوّل هو الإدعاء، ويمثّله المضرور من الجريمة، والآخر هو مرتكب الجريمة، ويقع عبئ الاتهام أو الادعاء على عاتق المجني عليه أو المضرور من الجريمة، كما لا شأن للسلطات العامة بجمع الأدلّة. وينحصر دور القاضي في هذا النظام في فحص الأدلة المقدمة من كل منهما، والموازنة فيما بينها، ومن ثمّ الحكم لمصلحة من ترجح أدلته دون أن يكون من سلطته المبادرة إلى اتخاذ أي إجراء يراه ضروريا لكشف الحقيقة[4][5]. أمّا إذا كان النظام

---

[1] د/ محمود نجيب حسني، المرجع السابق، ص 78.

[2] وتكمن العلّة في الفرق بين دور كل من القاضي الجنائي والقاضي المدني في البحث عن الأدلة، إلى اختلاف طبيعة المصالح التي تحميها كل من الدعوى الجنائيّة والدعوى المدنيّة، فالأولى تحمي مصلحة عامة هي مصلحة المجتمع، أمّا الدعوى المدنيّة فإنّها تحمي مصالح خاصّة بأطرافها. انظر: د/ محمد زكي أبو عامر، الإجراءات الجنائيّة، ص 851.

[3] وفي ذلك قضت محكمة النقض المصريّة " أنّ القانون قد أمدّ القاضي في المسائل الجنائيّة بسلطة واسعة وحريّة كاملة في سبيل تقصّي ثبوت الجرائم أو عدم ثبوتها والوقوف على حقيقة علاقة المتهمين ومقدار اتصالهم بها ففتح له باب الإثبات على مصراعيه يختار من كل طرقه ما يراه موصلا إلى الكشف عن الحقيقة ويزن قوّة الإثبات المستمدّة من كل عنصر بمحض وجدانه فيأخذ بما تطمئن إليه عقيدته ويطرح ما لا ترتاح إليه غير ملزم بأن يسترشد في قضائه بقرائن معيّنة بل له مطلق الحريّة في تقدير ما يعرض عليه منها ووزن قوّته التدليلية في كل حالة حسبما يستفاد من وقائع كل دعوى وظروفها، بغيته الحقيقة التي ينشدها إن وجدها ومن أي سبيل يجده مؤديا إليها ولا رقيب عليه في ذلك غير ضميره وحده. نقض 12 يونيه 1936، مجموعة القواعد القانونيّة، الجزء الرابع، رقم 406، ص 575. نقض 20 يناير 1969، مجموعة أحكام النقض، س 20، رقم 35، ص 164.

[4] Merle et Vitu، op.cit، n° 111، p. 171.

[5] لمزيد من التفصيل حول النظام الاتهامي والأسس التي يقوم عليها، انظر: د/ عبد الوهاب العشماوي، الاتهام الفردي أو حق الفرد في الخصومة الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1953، ص 53 وما بعدها.

التنقيبي (Le procédure inquisitoire) هو المهيمن على الإجراءات الجنائيّة كالقانون الفرنسي والجزائري والمصري فحينئذ يكون دور القاضي إيجابيا في صدد تحقيق الدعوى والفصل فيها، ذلك أنّ الضرر الذي تحدثه الجريمة ليس ضررا فرديا فحسب، وإنّما أضحى ضررا عاما يهدّد مصلحة المجتمع في أمنه واستقراره وسلامته، لذلك كان من الضروري منح القاضي السلطات اللازمة للوصول إلى الحقيقة الفعليّة في الدعوى المنظورة أمامه [1].

وتجدر الإشارة أنّ المقصود بالقاضي ليس هو قضاء الحكم فحسب، وإنّما يشمل أيضا قضاء التحقيق باعتبار أنّ مشكلة الإثبات قد تثور في أيّ مرحلة تمرّ بها الدعوى الجنائيّة بل يمكن أن تثور قبل ذلك أي في مرحلة جمع الاستدلالات أيضا.

2 ـ **مظاهر الدور الايجابي للقاضي الجنائي في توفير الدليل الالكتروني:** إذا كانت مهمّة البحث عن الأدلة وتقديمها في مرحلة المحاكمة تقع بصفة أساسيّة على عاتق الإدعاء والدفاع، فلا يعني ذلك أنّ القضاة لا يتحمّلون جانبا من هذه المسؤوليّة. بلْ يلقى عليهم عبء الإثبات شأنهم في ذلك شأن سلطة الاتهام، وللاستدلال على ذلك نلاحظ أنّ المحاكم الفرنسيّة في مواد الجنح والمخالفات يمكنها أن تتخذ جميع الإجراءات الضروريّة لتكوين اقتناعها [2]، فلها أن تسأل أو تستجوب المتهم حول أساس الاتهام الموجه إليه(المادتان 442 و536) من قانون الإجراءات الجنائيّة الفرنسي، ويمكنها سماع الشهود أو استدعاء الخبراء إذا واجهتها مسألة فنيّة.

أمّا في مواد الجنايات فقد أفرد القانون الإجرائي الفرنسي نصّا خاصّا منح بموجبه رئيس محكمة الجنايات سلطة تقديريّة خاصّة للقيام بجميع الإجراءات التي يقدّر فائدتها في كشف الحقيقة(المادة 310) من قانون الإجراءات الجنائيّة الفرنسي.

ولا يختلف الوضع في ذلك عن القانون المصري، فقد نصّت المادة 291 من قانون الإجراءات الجنائيّة على أنه "للمحكمة أن تأمر، ولو من تلقاء نفسها أثناء نظر الدعوى بتقديم أي دليل تراه لازما لظهور الحقيقة"، ولهذا أجيز للمحكمة أن توجه إلى الشهود أيّ سؤال ترى لزومه لظهور الحقيقة في أيّة حالة كانت عليها الدعوى [3]، وسمح لها أن تسمع شهادة أيّ شخص يحضر من تلقاء نفسه لتقديم ما لديه من معلومات في شان الدعوى المعروضة [4]. وأن

---

(1) د/ أحمد عوض بلال، الإجراءات الجنائيّة المقارنة، والنظام الإجرائي في المملكة العربيّة السعوديّة، دار النهضة العربيّة، القاهرة، 1991، ص 91 .

(2) د/ السيد محمّد حسن شريف، النظريّة العامة للإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 2002، ص 213.

(3) المادة 273 من قانون الإجراءات الجنائيّة المصري.

(4) المادة 277 من قانون الإجراءات الجنائيّة المصري.

تأمر ولو من تلقاء نفسها بإعلان الخبراء ليقدموا إيضاحات بالجلسة عن التقارير المقدّمة منهم في التحقيق الابتدائي أو أمام المحكمة[1]. وإذا تعذّر تحقيق دليل أمام المحكمة، جاز لها أن تندب أحد أعضائها أو قاضيًا آخر لتحقيقه[2]. كذلك يعدّ من مظاهر الدور الايجابي للقاضي الجنائي في القانون المصري ما نصّت عليه المادة(274) من قانون الإجراءات الجنائيّة، حيث حظرت استجواب المتهم ما لم يقبل هو بذلك، غير أنها أضافت أنّه إذا ظهر أثناء المرافعة والمناقشة بعض الوقائع ترى لزوم تقديم إيضاحات عنها من المتهم لظهور الحقيقة يلفته القاضي إليها ويرخص له بتقديم تلك الإيضاحات.

وتطبيقا على الجرائم الالكترونيّة، فإنّ القاضي الجنائي يستطيع من أجل الوصول إلى الحقيقة أن يوجه أمرا إلى مزود خدمة الانترنت بتقديم بيانات معلوماتيّة المتعلّقة بمستخدم الانترنت، كعناوين المواقع التي زارها ووقت الزيارة والصفحات التي اطلع عليها والملفات التي جلبها والحوارات التي شارك فيها والرسائل الالكترونيّة التي أرسلها أو استقبلها وغيرها من المعلومات المتعلقة بكل أفعال المستخدم عندما يتّصل بالشبكة.

ومن مظاهر الدور الايجابي للقاضي الجنائي في البحث عن الدليل الالكتروني، أنّه بإمكان القاضي الجنائي أن يأمر القائم بتشغيل النظام بتقديم المعلومات اللازمة لاختراق النظام والولوج إلى داخله، كالإفصاح عن كلمات المرور السريّة والشفرات الخاصة بتشغيل البرامج المختلفة، أو تكليفه بحل رموز لبيانات مشفّرة داخل ذاكرة الحاسب الآلي، كذلك للقاضي الجنائي سلطة الأمر بتفتيش نظم الحاسب الآلي بمكوناته الماديّة والمعنويّة وشبكات الاتصال[3] متى ما قدّر ضرورة وملائمة هذا الإجراء.

وحيث أنّ للخبرة في مجال المساعدة القضائيّة دورا كبيرا، فهي تعدّ من أقوى مظاهر تعامل قاضي الموضوع مع الواقعة الإجرامية المعروضة، وهذا الأخير يملك ندب خبراء، لاسيما وأنّ الأصل يظلّ للتحقيق الذي تجريه المحكمة في الجلسة[4]، وهذا ما أكّدته المادة (292) من قانون الإجراءات الجنائيّة المصري حينما نصّت على " للمحكمة سواء من تلقاء نفسها أو بناء على طلب الخصوم أن تعيّن خبيرا واحدا أو أكثر في الدعوى". وفي مجال البحث عن الدليل الالكتروني نجد أنّ الخبرة التقنيّة تعدّ من أقوى مظاهر التعامل القانوني والقضائي مع ظاهرة تكنولوجيا المعلومات، فهي تؤدي دورا لا يستهان به خاصّة مع نقص المعرفة القضائيّة الشخصيّة لظاهرة الحاسب الآلي والانترنت، فمثلا البحث عن معلومات

---

(1) المادة (293) من قانون الإجراءات الجنائيّة المصري.

(2) المادة (294) من قانون الإجراءات الجنائيّة المصري.

(3) انظر فيما سبق، ص 54 وما بعدها .

(4) د/ أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائيّة، المرجع السابق، ص 487.

داخل جهز الحاسب الآلي ذاته يعدّ أمرا بالغ التعقيد ويحتاج إلى وجود خبير لاسيما في حالة التشفير وغيرها من الوسائل الفنيّة.

ب - الدور الايجابي للقاضي الجنائي في قبول الدليل الالكتروني: تحدثنا فيما سبق عن الدور الايجابي للقاضي الجنائي في توفير الدليل الالكتروني، من حيث ماهيته ومظاهره، وتبيّن كيف أنّ القاضي الجنائي على خلاف القاضي المدني، حيث لا يجوز له أن يقنع بما يقدمه له الأطراف في الدعوى من أدلّة، وإنّما عليه أن يبحث بنفسه عن الأدلّة ذات الأثر في تكوين عقيدته، وأن يستثير الأطراف إلى تقديم ما لديهم من أدلّة، وتعدّ مرحلة قبول الدليل الالكتروني الخطوة الثانيّة بعد البحث عن الدليل وتقديمه من قبل كلّ من سلطة الادعاء والمتهم والقاضي في حالة ما إذا تطلب أنّ الفصل في الدعوى يتطلب تحقيق دليل بعينه، وذلك من أجل خلق حالة اليقين المطلوبة لدى القاضي كأساس لإصدار حكمه بالإدانة أو لتأكيد حالة البراءة.

وتجدر الإشارة في هذا الصدد أنّ القاضي الجنائي أوّل ما يتأكد منه في هذه المرحلة ــ مرحلة قبول الدليل ــ هو مدى مشروعيّته(الدليل الالكتروني)، وذلك قبل الوصول إلى المرحلة الأخيرة ألا وهي مرحلة تقدير الدليل، لأنّ القاضي الجنائي لا يقدّر إلا الدليل المقبول، ولا يكون كذلك إلا إذا كان مشروعاً.

الفرع الثاني
في النظام الأنجلوأمريكي

أساس مشكلة قبول الدليل الالكتروني في الإثبات الجنائي:

نظام الإثبات في التشريعات ذات الأصل الأنجلوأمريكي يختلف عن غيره من التشريعات التي تأخذ بالنظام اللاتيني، فالدليل في النظام الأوّل تحكمه قواعد خاصة لقبوله أمام المحاكم، سواء تعلّقت هذه القواعد بمضمون أو فحوى الأدلة، أو بكيفيّة تقديم الأدلة.

فمن بين القواعد المتعلّقة بمضمون الأدلة: قاعدة استبعاد **شهادة السماع (The Hearsay Rule)** [1]، ومادام الدليل الالكتروني في أصله يمثّل شهادة سماع على أساس أنّه يتكوّن من جمل وكلمات أدخلها شخص إلى جهاز الكمبيوتر، سواء تمّ معالجة تلك البيانات أو لم يتمّ ذلك.

ومن شأن ذلك أن يثير اعتراضا على قبول المستندات المطبوعة التي يخرجها الحاسوب في الإثبات أمام القضاء الجنائي.

---

[1] Thomas J. Gardner, Terry M. Anderson, Criminal Evidence, Principles and cases, (5) fifth edition, Thompson Wadsworth Publisher, 2004، p.140.

أمّا بالنسبة للقواعد المتعلقة بكيفيّة تقديم الأدلة إلى القضاء، وتحديد مدى قبولها، كأدلة إثبات في المواد الجنائيّة، تلك القاعدة المعروفة **بقاعدة الدليل الأفضل (The Best Evidence Rule)**، أو **قاعدة المحرّر الأصلي(Original Document Rule)**، ولو طبّقنا هذه القاعدة من حيث المبدأ على الدليل الالكتروني لكان مستبعدا كوسيلة إثبات في هذا النظام. وهو ما أدّى إلى قلق رجال الضبط القضائي والمدّعيين العموميين من أنّ مجرّد مخرجات طابعة ملف الكتروني مخزّن على الحاسوب لا يعدّ أصليّا[1].

ويرجع السبب في ذلك إلى أنّه غالبا ما يعرض الدليل الالكتروني أمام القضاء في شكل مستندات مطبوعة أو كبيانات معروضة على شاشة الكمبيوتر، والأصل في الدليل الالكتروني أنه مجرّد إشارات الكترونية ونبضات ممغنطة، ليست مرئيّة للعين البشرية، ممّا لا تتيح للمحلفين أو للقاضي مناظرة أو وضع أيديهم على الدليل الأصلي، وما يقدّم إليهم من وثائق أخرجها الحاسوب، سوى **نسخ لأصول** ممّا يجعله **دليلا ثانويا لا أصليّا**. فضلا عن ذلك أن النسخة لا تُظهر جميع البيانات المتضمّنة في الأصل، فعلى سبيل المثال الوثيقة المطبوعة من وثائق مايكروسوفت وورد (Microsoft word) لا تُظهر جميع التعديلات والملاحظات في حالة ما إذا تمّ فيها تغيير الوثيقة الأصليّة[2]. بالإضافة إلى ذلك أنّ الأصول في بعض العمليات التي تجرى عن طريق الحاسب قد لا تعود موجودة، وربّما لم يكن لها وجود أصلا، كما في حالة التحليلات أو الإسقاطات المعالجة[3].

وعلى ذلك، نخلص أنّ هناك قاعدتين مهمّتين تحكمان الإثبات الجنائي في النظام الانجلو أمريكي، قاعدة استبعاد شهادة السماع، وقاعدة الدليل الأفضل، والإشكال الذي ينبغي طرحه في هذا المقام هو:

ما موقع الدليل الالكتروني من هذه القواعد، فهل يتمّ رفضه ومن تمّ استبعاده كدليل إثبات جنائي، أم يتمّ قبوله، وعلى أيّ أساس يكون هذا القبول؟. وهو ما سنحاول بيانه في النقاط التاليّة:

أوّلا ـ الدليل الالكتروني مقبول استثناء من قاعدة استبعاد شهادة السماع:

الشهادة قد تكون عن رؤية (حضوريّة)، وقد تكون شهادة سماعيّة يشهد فيها الشاهد بما سمعه ممّن رأى الواقعة، والحقيقة أنّ بعض التشريعات كالولايات المتحدة الأمريكيّة وانجلترا

---

[1] د/ عمر محمّد بن يونس، الإجراءات الجنائيّة عبر الانترنت في القانون الأمريكي، المرجع السابق، ص 440.

[2] Eoghan Casey, op –cit, p 135.

[3] د/ هشام محمد فريد رستم، الجوانب الإجرائيّة للجرائم المعلوماتيّة، المرجع السابق، ص 173.

وكندا واستراليا لا تعتدّ بالشهادة السماعيّة في الإثبات الجنائي. وبما أنّ الدليل الالكتروني يعدّ شهادة سماع[1]، فيعتبر من أوّل وهلة أنّه دليل غير مقبول، إلا أنّه في الحقيقة غير ذلك، لأنّ المشرع في الأنظمة الأنجلوأمريكية وضع قائمة من الاستثناءات على قاعدة شهادة السماع ومن بينها البيانات والمعلومات التي يتمّ الحصول عليها من الكمبيوتر (Evidence from Computer) أو (Computer Printouts)، حيث يكون هذا الأخير مقبولا في الإثبات شأنه شأن غير من الأدلة، لكن بشروط معيّنة، وذلك ما سنحاول التعرّض إليه فيما يلي:

أ ـ مدى اعتبار الدليل الالكتروني شهادة سماع: سنتناول تحديد مفهوم شهادة السماع بداية، ثمّ بيان أهم الاستثناءات الواردة على هذه القاعدة ومنها الدليل الالكتروني، وأخيرا موقف القضاء الانجليزي من أساس قبول هذا الدليل، لأنه كان هناك نوع من الاشتباه في تكييف الدليل الالكتروني بين اعتباره شهادة مباشرة أو شهادة غير مباشرة (شهادة سماع).

ـ مفهوم شهادة السماع: يقصد بشهادة السماع أو كما يطلق عليها البعض التسامع عن الغير[2] أو الشهادة النقليّة[3] وبالانجليزيّة "Hearsay"[4]: بيان أو تقرير شفوي أو كتابي يحدث خارج المحكمة، ويقدّم إليها من أجل الحقيقة أو بعبارة أخرى من أجل إثبات أمر حدث خارج الجلسة وكان صادقا[5][6].

ويرى البعض من الفقهاء[7] أنّ شهادة السماع نوع من الشهادة غير المباشرة, وليست هي شهادة السماع ذاتها, حيث تقسّم الشهادة غير المباشرة إلى نوعين, "الشهادة السماعيّة" و"الشهادة بالتسامع", وتعني الأولى أنّ شخصا سمع من آخر معلومات عن الواقعة محل التحقيق, كما في الحالة التي يشهد فيها الشخص بأنّه سمع من آخر أنه أنّه شاهد على

---

(1) انظر فيما سيأتي، ص 128.

(2) د/ رمزي رياض عوض، حماية المتّهم في النظام الأنجلوأمريكي، دار النهضة العربيّة، القاهرة، 1998، ص 33.

(3) د/ فرج إبراهيم العدوي عبده، سلطة القاضي الجنائي في تقدير الأدلّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1995، ص 205.

(4) Alan Taylor. BA(Bristol), M Phil(Oxon), Principles of Evidence, Cavendish Publishing Limited, Second Edition, London, Sydney, 2000, p. 164.

(5) د/ رمزي رياض عوض، المرجع السابق، ص 33.

(6) مثال عن شهادة السماع: "أنّ السيّدة (س) قالت لي السيدة (ص) قد اغتصبها بعد الحفلة المدرسيّة الراقصة"، فهذا القول حدث خارج المحكمة، ولم يقدّم من السيّدة ذاتها، وأنّ السيّدة (س) قدّمته للمحكمة من أجل مسألة معيّنة في الدعوى يثار الجدل بشأنها، وهي أنّ (أ) شخص مغتصب. هذا المثال مشار إليه عند: د/ رمزي رياض عوض، نفس المرجع، ص 34.

(7) د/ أمين مصطفى محمّد, حماية الشهود في قانون الإجراءات الجنائيّة, دراسة مقارنة, دار النهضة العربيّة, القاهرة, 2008, ص 16.

ارتكاب المتهم للجريمة, أما "الشهادة بالتسامع", فهي مجرّد ترديد لإشاعة تتردّد بين الناس بدون الجزم بصحتها, فقد تكون صادقة أو لا تكون, وترجع العلّة في التمييز بين النوعين, في أنّ النوع الأول من الشهادة له قوة في الإثبات, ولكنّها بدرجة أقل من النوع الثاني والتي لاتصلح أساسا كدليل لاستحالة التحقق من صحتها[1].

وإن كان البعض الآخر من الفقه[2], يّرجّح التساوي بين مصطلح شهادة غير المباشرة وشهادة سماع.

وانطلاقا من ذلك, يتداول بصفة عامة عن شهادة السماع وهي التي تهمّنا في هذا الموضوع تعريفان أساسيان[3]:

الأوّل هو ما قال به (Professor Wigmore)، والثاني، قدّمه (Morgan). ويجري التعريف الأوّل على أنّ شهادة السماع هو دليل شفوي أو مستندي يقدّمه شخص ما إلى المحكمة، محمولا على أنّه عبارات أو سلوك صدر من آخر خارج المحكمة، ويتوقّف قبوله أو استبعاده على مقدار الثقة التي تتوافر لدى المحكمة فيمن أدلي به خارج المحكمة.

أمّا التعريف الثاني، والذي قدّمه (Morgan)، فقد قال فيه أنّ:" شهادة السماع هو دليل يقدّم من خلال شخص نقلا لعبارات أو سلوك صدر خارج المحكمة من شخص آخر، ويؤكّد أو لا يؤكّد مسألة معيّنة لإثبات الحقيقة في تلك المسألة، ويعتقد من يقدّمه في صحتّه".

والفارق بين التعريفين الأخير يجعل من شهادة السماع دليلا غير حازم (Non assertive)، بمعنى مجرّد دلالة، لا يرتق لمستوى الدليل[4]، وهذا التعريف هو السائد حاليّا معظم التشريعات التي تأخذ بالنظام الأنجلوأمريكي.

والأصل في شهادة السماع أنّها لا يعوّل عليها كدليل، حيث يمكن الحكم على مقتضاه، ويرجع السبب في ذلك إلى عدم الثقة في الشخص الذي يدلي به خارج المحكمة. فهو لا يؤدّي يمينا أمام المحكمة، حتّى يخضع لملاحظة القاضي أو المحلّف وقت إدلائه أو كتابته، ومن ناحية أخرى فإنّ هذا السبيل لا يتيح للمتّهم حقوقه الدستوريّة، خاصة حق المتّهم في المواجهة.

---

(1) د/ أمين مصطفى محمّد, نفس المرجع, ص 17.

(2) د/ رمزي رياض عوض، المرجع السابق, ص 33. كذلك: د/ فرج إبراهيم العدوي عبده, المرجع السابق, ص 205 وما بعدها.

(3) Joseph (D). Schloss، Evidence and its Legal Aspect، printed in United States of America، published by Charles E. Merrill Publishing Co، 1976، p. 291.

(4) د/ رمزي رياض عوض، المرجع السابق، ص 34.

ومع ذلك، لا تعني هذه القاعدة أن يكون النقل عن الغير، سواء كان نطقا أو كتابة يتمّ تجاهله نهائيّا، بل هناك حالات استثنائيّة يتمّ فيها قبول شهادة السماع كدليل في الدعوى الجنائيّة. وأهم هذه الحالات هي:

- أقوال المجني عليه التي نطق بها قبل وفاته(Dying Declaration) .
- إخبار أحد أعضاء الاتفاق الجنائي (Admission of co. Conspirator).
- التسجيلات الرسمية.
- البيانات والمعلومات التي يتمّ الحصول عليها من الكمبيوتر (Evidence from Computer)
- التذكر الماضي بالوقائع (Past recollection).
- التقرير التلقائي (Spontaneous Statement).
- النطق بمفهوم الانطباعيّة (Declaration of present sense impression).

ويتبيّن من خلال ما سبق أنّ الدليل الالكتروني يدخل في طائفة الحالات الاستثنائيّة عن قاعدة شهادة السماع، ليصبح هذا الدليل مقبولا في الإثبات الجنائي.

وتجدر الإشارة إلى أنّ قبول الدليل الالكتروني على أساس استثناء قاعدة شهادة السماع لا ينطبق على جميع أنواع سجلات الحاسوب، ذلك أنّه سبق ذكر[1] أنّ هذه الأخيرة تمّ تقسيمها من قبل المحاكم الفدراليّة الأمريكيّة إلى ثلاث أنواع، **سجلات الحاسوب المخزنة(Computer-stored records)**، **وسجلات الحاسوب المتوالدة-Computer (generated records)**، وهناك نوع ثالث من السجلات يجمع **بين التدخل الإنساني و معالجة الكمبيوتر.**

ففي النوع الأوّل، حيث تحتوي سجلات الحاسوب المخزّنة على بيانات بشريّة، مثل المخرجات من برنامج الكتابة من الكمبيوتر(Word). فهي تعتبر شهادة سماعيّة مثلها في ذلك مثل الكلمات أو التقريرات التي يسجّلها الإنسان على الأجهزة المختلفة[2].

أمّا النوع الثاني، فإنّ الجهاز هو الذي يقوم بتدوين البيانات التي تصلح أن تقدّم مباشرة إلى المحكمة، فهي ليست من قبيل شهادة السماع، وتتوقف قيمته الثبوتيّه على ما إذا كان جهاز الكمبيوتر يعمل بطريقة أم لا [3].

---

(1) انظر فيما سبق، ص 43 وما بعدها .

(2) د/ عمر محمّد بن يونس، المرجع السابق، ص 437 وما بعدها. وانظر أيضا د/ شيماء عبد الغني، المرجع السابق، ص 403.

(3) د/ عمر محمّد بن يونس، المرجع السابق، ص 422.

أمّا بالنسبة للنوع الثالث، والذي يجمع بين التدخل الإنساني ومعالجة الكمبيوتر، وإن كان جزء منها يعد شهادة السماع وهو الصادر عن الإنسان إلا أنه لا يعدّ هذا النوع من السجلات شهادة سماع، حتّى وإن كان يجب توافر لصحّة المستند الالكتروني شرطين: فمن ناحية يجب توافر الشرط اللازم لصحة الشهادة السماعيّة، كما أنّه يجب التأكد من عمل الجهاز نفسه على نحو صحيح.

ب ـ موقف القضاء الانجليزي من أساس قبول الدليل الالكتروني في الإثبات الجنائي:

إذا كان المشرّع الانجليزي قبل الدليل الالكتروني في الإثبات الجنائي على أساس أنّه استثناء شهادة السماع، إلاّ أنّ القضاء قد قبل هذا الدليل على أساس أنّه شهادة مباشرة، ويظهر ذلك جليّا في العديد من القضايا المعروضة أمامها، ففي قضيّة (R.v.Wood)[1] تمّ العثور في حيازة المتّهم على بعض المعادن التي قد سرقت وكانت تركيبة المادة الكيميائيّة لهذه المعادن مسجّلة في كمبيوتر المجني عليه، وقد قدّمت ورقة مخرجة من الكمبيوتر كدليل، والسؤال الذي طرح في هذه القضيّة هل تعتبر هذه الورقة الناتجة عن الكمبيوتر دليلا سماعيّا، وبالتالي لا نأخذ به؟ ــ أجابت عن ذلك المحكمة معتبرة أنّ الورقة الناتجة عن الكمبيوتر مقبولة وفقا للشريعة العامة، وتصلح للإثبات فهي ليست من قبيل الشهادة السماعيّة. كما قبلت المحكمة الجزئيّة في قضيّة (Castle v. Cross)[2] الدليل المستخرج من جهاز قياس نسبة الكحول في الدم باعتباره دليلا مباشرا وليس من قبيل الشهادة السماعيّة.

وفي نفس الاتجاه أيضا قضت محكمة الاستئناف في انجلترا بقبول الدليل المستخرج من الكمبيوتر في قضيّة (R.v.Pettigrew)[3] بوصفه شهادة مباشرة وليست سماعيّة والتي تخلص وقائعها في أنّه وجد في حيازة المتّهم الذي قام بالسطو على البنك أرقام النقود المسروقة والتي كانت مسجّلة في كمبيوتر البنك في انجلترا، وقد قبلت المحكمة في هذه القضيّة مخرجات الكمبيوتر الورقيّة باعتبارها دليلا مباشرا وليس من الأدلة السماعيّة.

ثانيا ـ الدليل الالكتروني مقبول استثناء من قاعدة الدليل الأفضل:

تذهب قواعد الإثبات في التشريعات ذات الأصل الأنجلوأمريكي إلى تطبيق قاعدة الدليل الأفضل والتي يقصد بها: لأجل إثبات محتويات كتابة أو سجل أو صورة، فإنّ أصل الكتابة

---

[1] R.v.Wood، 1983، 76 Cr. App. R 23، Steve Uglow، evidence، text and materials، London، Sweet and Maxwell، 1997، p. 514

مشار إليه عند: د/ شيماء عبد الغني، المرجع السابق، ص 391.

[2] Castle v. Cross، 1985، 1 All E.R،87 Steve Uglow، ibidem، p.515.

[3] وقائع هذه القضيّة مستمدّة من: Steve Uglow , ibid. P.514.

أو السجل أو الصورة يكون مطلوبا [1]. بمعنى لا يجوز تقديم الصورة لإثبات محتوى الأصل[2]. بصفة عامة حين يقدّم أحد الأطراف، تأييدا لدعواه، دليلا يستند إلى عدّة دعائم، فإنّ عليه أن يقدّم أفضل نموذج، وهو ما يعني أن تكون الأدلة الواجب تقديمها أوليّة وليست ثانويّة، أصليّة لا بديلة، وأن يكون الدليل المقدّم هو أفضل ما يتاح الحصول عليه بالنسبة لطبيعة وظروف القضيّة[3].

وقد قرّر القانون الأمريكي هذه القاعدة بموجب المادة (1002) من قانون الإثبات الأمريكي والتي تقضي على أنّ حجيّة الكتابة أو التسجيل أو الصورة رهن بتقديم الأصل إلاّ إذا نصّ على خلاف ذلك، وقد جاء نصّها الحرفي كالتالي:" باستثناء ما هو مقرّر في هذا القانون أو بقانون خاص يصدر عن الكونجرس، فإنّه عند إثبات مضمون الكتابة والتسجيل والصورة فإنّه يلزم توافر **أصل الكتابة والتسجيل والصورة**"[4].

ومع ظهور المستندات الالكترونيّة استدعى الأمر إلى تغيير هذه القاعدة لكي تتلاءم مع عصر المعلومات، وقد استجابت بعض التشريعات(كالقانون الأمريكيّ والانجليزي) لهذه المستجدات، وقام بحسم هذه المسألة لصالح الدليل الالكتروني، وذلك من خلال تعديل قانون الإثبات الفدرالي الأمريكي[5]،والدليل على ذلك أنّه تمّ تطوير المادة(1/101) من قانون الإثبات

---

[1] د/ عمر محمّد بن يونس، المرجع السابق، ص 440.

[2] Amoury (B) et Poullet (Y)، le droit de la preuve face à l'informatique et télématique، revue internationale de droit comparé، n° 2، avril - juin، 1985، p. 339.

[3] Bologna (Jack)، Corporate Fraud، the basics of prevention and detection، Butterworth Publishers، 1984، p. 75.

مشار إليه عند : د/ هشام محمد فريد رستم، المرجع السابق، ص 171. ولمزيد من التفاصيل حول قاعدة الدليل الأفضل انظر الموقع التالي:

http://media.hypersites.com/clients/989/filemanager/articles/articl11.pdf

[4] **Rule (1002).of FEDERAL RULES OF EVIDENCE**، provides that: **" To prove the content of a writing، recording، or photograph، the original writing، recording، or photograph** is required، except as otherwise provided in these rules or by Act of Congress".

[5] ينبغي التنبيه أنّ التطور الذي حصل في مجال التشريع لا يقتصر فقط على قواعد الفدراليّة للإثبات الأمريكي، بل يشمل فضلا عن ذلك القوانين الخاصة بالولايات كتلك القائمة في ولاية **كاليفورنيا**، وايوا، حيث تنص المادة (5/1500) من قانون الإثبات الكالفورني، على أنّ:" المعلومات المسجّلة بواسطة الحاسب أو برامج الحاسب، أو نسخ أيّهما لا يجب وصفها أو معاملتها على أنها غير مقبولة بمقتضى قاعدة "أفضل الأدلّة" ". وكذلك جاءت المادة (16/716) من القانون الجديد لجريمة الحاسب لسنة 1984 بولاية ايوا(Iowa)، قاعدة إثبات جديدة تقضي بأنّه :" في أحوال الاتهام بمقتضى هذا الفصل، تكون مخرجات الحاسب مقبولة كدليل على الكيان المنطقي أو البرنامج أو البيانات التي يحتويها حاسب أو البيانات التي تؤخذ منه، بغض النظر عن تطبيق قاعدة لإثبات تقضي بخلاف ذلك".

الأمريكي[1] لكي تشمل الدليل الالكتروني بشكل موسّع، حيث سمحت بالاعتراف بالمواد المكتوبة (Writings) والمسجّلة (Recording) والالكترونيّة(Electronic)، لكي تحظى بذات الاهتمام الذي تحظى به الأدلّة الأخرى في المحاكم، وبالتالي قام المشرّع الأمريكي باستخدام مدلول موسع للكتابة والتسجيلات ليشمل كل من الحروف أو الكلمات أو الأرقام أو ما يعادها، مكتوبة على اليد أو منسوخة على الآلة الكاتبة أو مطبوعة أو تمّ تصويرها أو اتخذت شكل نبضات مغناطيسيّة بتسجيل ميكانيكي أو الكتروني أو أيّ شكل آخر من تجميع المعلومات.

لذلك يتمّ اعتبار الكتابة الموجودة داخل الجهاز في صورة كهرومغناطيسيّة من قبيل النسخة الأصليّة وبالتالي لا نصطدم بقاعدة الدليل الأفضل، ونعتبر أنّ المحرّرات الالكترونيّة نسخة أصليّة. ولقد ذهب القانون الأمريكي أبعد من ذلك حال توسّعه في مدلول عرض الدليل الالكتروني، إذ تنص المادة(1001/ 3 من قانون الإثبات الأمريكي) على أنّه:" **إذا كانت البيانات مخزّنة في حاسوب أو جهاز مماثل فإنّ مخرجات الطابعة أو أيّة مخرجات أخرى يمكن قراءتها بالنظر إلى ما تمّ إظهارها وتبرز انعكاسا دقيقا للبيانات، تعدّ بيانات أصليّة**"[2]. ويفهم من خلال هذه المادة أنه يقبل الدليل الالكتروني المستخرج من الطابعة كدليل أصلي كامل، من غير جلب الحاسوب إلى قاعة المحكمة لتأكيد تلك الأصالة.

فضلا عن ذلك فقد توسّع القانون الأمريكي أكثر حين قيامه باعتماد مقياس القانون العام **(Commen Law)**، وذلك في إطار الاعتراف بالنسخة طبق الأصل(Duplicate) الفوريّة الصادرة عن الحاسوب، فالمادة (4/1004) من قانون الإثبات الأمريكي تعرّف النسخة طبق الأصل بأنّها: " **النسخة المطابقة للأصل المنتجة لذات الأثر للنسخة الأصل، ..عن طريق إعادة تسجيلها ميكانيكيّا أو الكترونيا ..أو عن طريق وسيلة تقنيّة أخرى مساوية**

---

[1] **Rule (1001 /1). of FEDERAL RULES OF EVIDENCE**، provides that:" Writings and recordings.—''Writings'' and ''recordings'' consist of letters، words، or numbers، or their equivalent، set down by handwriting، typewriting، printing، Photostatting، photographing، magnetic impulse، mechanical or electronic recording، or other form of data compilation"

[2] **Rule(1001 / 3). of FEDERAL RULES OF EVIDENCE**، provides that:" If data are stored in a computer or similar device، any printout or other output readable by sight، shown to reflect the data accurately، is an ''**original**'' .

التي تعيد إنتاجها بدقّة كالأصل" [1] [2].

والقانون الأمريكي يقرّر في المادة (1003) من قانون الإثبات الأمريكي، أنّ **"النسخة المطابقة للأصل تقبل كالأصل إلاّ إذا: أولاً: أثيرت حولها تساؤل جدّي يتعلّق بجديّتها وأصالتها، ثانيًا: إذا كانت الظروف لا تسمح بقبول النسخة المطابقة للأصل لكي تحلّ محلّ الأصل"** [3]..

أمّا بالنسبة للقانون الانجليزي فقد تمّ قبول صور المستندات أو جزء منها بموجب المادة(27) من قانون العدالة الجنائيّة لسنة 1988،

ثالثا ـ شروط قبول الدليل الالكتروني في الإثبات عند النظام الانجلو أمريكي:

تعاقبت القوانين في انجلترا التي أصبحت تسمح بقبول الدليل الإلكتروني المتولّد من معالجة الكمبيوتر منذ قانون الإثبات الجنائي لسنة 1968، وحتّى القانون الصادر في 1988الخاص بقانون العدالة الجنائيّة، مرورا بقانون الشرطة والإثبات الجنائي سنة 1984. وقد ترتّب على ذلك قبول المشرّع الانجليزي للدليل الالكتروني كدليل في الإثبات الجنائي، وذلك خروجا عن الأصل العام الذي يتبنّاه القانون الانجليزي في عدم قبول الشهادة السماعيّة، إلاّ أنّ هذا القبول مقيّد بشروط معيّنة نصّت عليها المادة (69) من قانون الشرطة والإثبات الجنائي لسنة 1984 وهي كالتالي:

1ـ عدم وجود أسباب معقولة للاعتقاد بأنّ البيان يفتقر إلى الدقة بسبب الاستخدام غير المناسب أو الخاطئ للحاسب.

---

(1) **Rule(1001/ 4)of FEDERAL RULES OF EVIDENCE،** provides that :"A duplicate'' is a counterpart produced by the same impression as the original، or from the same matrix، or by means of photography، including enlargements and miniatures، or by mechanical or electronic re-recording، or by chemical reproduction، or by other equivalent techniques
which accurately reproduces the original".

(2) وقد عرّفت المنظمة الدولية لأدلة الحاسوب (IOCE)of International Organization) **النسخة المطابقة للأصل** بأنّها" نسخة رقمية دقيقة لكل البيانات أو المعلومات الموجودة في البنود الأصليّة" :
- **Duplicate Digital Evidence** is "an accurate digital reproduction of all data objects contained on the original physical item".

(3) **Rule(1003)of FEDERAL RULES OF EVIDENCE،** provides that :" A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original".

2 ـ أنّ الحاسب كان يعمل في جميع الأحوال بصورة سليمة، وإذا لم يكن كذلك، فإنّ أيّ جزء لم يعمل فيه بصورة سليمة أو كان معطّلا عن العمل، لم يكن ليؤثّر في إخراج المستند أو دقّة محتوياته[1].

3 ـ الوفاء بأيّة شروط متعلّقة بالمستند محدّدة طبقا لقواعد المحاكمة(المتعلّقة بالطريقة أو الكيفيّة التي يجب أن تقوم بها المعلومات الخاصة بالبيان المستخرج عن طريق الحاسب).

وبناء عليه فإنّ النيابة العامة إذا استندت إلى مستند الكتروني في دعوى جنائيّة يتعيّن عليها أن تقدّم الدليل على أنّ الجهاز يعمل بطريقة صحيحة، ولا يلزم أن يتمّ إثبات هذه الأخيرة من جانب الخبير.

وقد أكّد القضاء الأمريكي هذا المعنى في قضيّة تلخص وقائعها في أنّ" متّهما بتجارة المخدرات كان يقوم بتسجيل الصفقات الممنوعة في ثلاثة ملفات في الكمبيوتر الخاص به تحت أسماء مستعارة، وقد حصل رجال الضبط القضائي على هذه الملفات بمساعدة المتّهم صاحب الكمبيوتر، وذلك عند تفتيش هذا الجهاز بناء على إذن بذلك، وقد تمّ ضبط ملفات تحتوي على أسماء المتعاملين مع المتّهم الأول". دفع أحد هؤلاء المتعاملين بعدم صحّة إجراءات الضبط وذلك لسهولة العبث بالبيانات وتغييرها وسهولة إدخال اسمه من المتّهم الأوّل. ومع ذلك رفضت المحكمة هذا الدفع مستندة إلى أنّه لا يشترط لصحّة إجراءات ضبط بيانات الكمبيوتر أن يتمّ من جانب الخبير[2].

---

[1] ويقيم القانون الكندي عدّة قرائن على سلامة عمل جهاز الكمبيوتر، تتمثل فيما يلي:

1 ـ إذا كانت الجهة صاحبة الجهاز تعتمد على الكمبيوتر في إدارة عملها اليومي، ومادام الجهاز يعمل بشكل صحيح فإنّ الملف الالكتروني يكون هو الآخر صحيحا، بل أكثر من ذلك فإنّ الملف يعتبر صحيحا أحيانا على الرغم من بعض الخلل في جهاز الكمبيوتر إذا كان هذا الخلل لا يؤثر في سلامة هذا الملف إذا لم توجد أسباب معقولة تدعو إلى التشكك في سلامة هذا الملف. (المادة 5 فقرة (a) من قانون الإثبات الالكتروني الموحّد في كندا).

2 ـ إذا تمّ تسجيل أو تخزين الملف الالكتروني من جانب شخص غير طرف في الدعوى القضائيّة في أثناء قيامه بأعماله المعتادة والذي لم يكن يعمل لحساب أحد أطراف تلك الدعوى الذي يحاول تقديمها في الدعوى.

3 ـ إذا قدّمها الخصم في دعوى أمام المحكمة وكان هذا المستند مستخرجا من جهازه، ذلك أنّه بتقديمه هذا المستند لصالحه إنّما يشهد بصحته.

[2] USA v. Whitaker، 127 F. 3d ، 595، 602(7th.Cir .1997).

ومن الواضح انّ صحّة الدليل الالكتروني يتوقف على صحّة برنامج التشغيل الذي يعمل الكمبيوتر بحسب تعليماته. ومن حق المتّهم أن تتاح له الفرصة لإثبات أنّ برنامج التشغيل لا يعمل بطريقة صحيحة أو منتظمة [1].

وتجدر الإشارة إلى أنّ قانون الشرطة والإثبات الجنائي لسنة 1984 لم يكتف بتحديد الشروط الواجب توافرها في مخرجات الحاسب كي تكون أدلّة مقبولة أمام القضاء، بل تضمّن كذلك توجيهات لكيفيّة تقدير قيمة أو وزن البيان المستخرج عن طريق الحاسب، فأوصت المادّة (11 من الجزء 2 من الملحق 3 من القانون المذكور) بمراعاة كل الظروف عند تقييم البيانات الصادرة عن الحاسب المقبولة في الإثبات طبقا للمادة (69 من القانون)، وبوجه خاص مراعاة "**المعاصرة**"، أي ما إذا كانت المعلومات المتعلّقة بأمر قد تمّ تزويد الحاسب بها في وقت معاصر لهذا الأمر أم لا، وكذلك مسألة ما إذا كان أيّ شخص من المتّصلين على أيّ نحو بإخراج البيان من الحاسب، لديه دافع لإخفاء الوقائع أو تشويهها[2].

---

[1] USA v. Moor، 923 F. 3d 910، 915(1th Cir. 1991).

[2] د/ هشام محمّد فريد رستم، المرجع السابق، ص 178.

المطلب الثاني

القيود الواردة على حريّة القاضي الجنائي في قبول الدليل الالكتروني

إذا كان من المسلم به أنّ للقاضي الجنائي حريّة الاستعانة بكافة وسائل الإثبات اللازمة بما في ذلك الدليل الالكتروني لتكوين عقيدته، فإنّه يثور التساؤل حول نطاق هذه الحريّة، وما إذا كانت حريّة مطلقة أو نسبية.

والواقع أنّ حريّة القاضي الجنائي في هذا الشأن لا يمكن أن تكون مطلقة من كل قيد، لأنّ السلطة المطلقة مفسدة مطلقة. لذا كان من الضروري رسم ضوابط وأطر معيّنة يتعيّن أن تمارس هذه السلطة في نطاقها بحيث لا تنحرف عن الغرض الذي يبغيه المشرع من ورائها، وهو الوصول إلى الحقيقة الفعلية في الدعوى، وإذا كانت هذه الحقيقة تمثل الهدف الأسمى لقانون الإجراءات الجنائيّة[1].

ونتيجة لذلك حدّدت أغلب التشريعات الأدلة التي تقبل في إثبات بعض الجرائم بحيث لا يجوز الإثبات بغيرها كأدلة إثبات جريمة الزنا، كما يتدخّل المشرع أحيانا لإلزام القاضي الجنائي بإتباع طرق الإثبات الخاصة التي تعرض عليه أثناء نظر الدعوى، مراعاة لطبيعة تلك المسائل من ناحيّة، وحتى لا يكون في نظرها أمام القاضي الجنائي هروب من الإجراءات المتبعة في مثلها أمام القضاء المختص (غير الجنائي)، من ناحية أخرى[2]، وسوف نلاحظ من خلال ذلك، مدى إمكانيّة القاضي الجنائي الاستعانة بالدليل الالكتروني لإثبات المسائل الأوليّة بمعنى الخروج عن الأصل.

على أنّ هناك قيدا عاما يحدّ من حريّة القاضي في قبول الدليل الالكتروني، هو قيد المشروعيّة حيث يشترط لكي يتمكّن القاضي من الاعتماد على دليل معيّن في الإدانة أن يكون قد تمّ الحصول عليه بطريقة مشروعة.

وعلى ضوء ما تقدّم، سوف نبيّن في الفرع الأول قيد مشروعيّة طريقة الحصول على الدليل الالكتروني، ثم نعرض في الفرع الثاني دراسة القيود المفروضة بمقتضى نصوص قانونيّة محدّدة، وذلك على النحو التالي .

---

[1] د/ السيد محمد حسن شريف، المرجع السابق، ص 246.

[2] د/ عبد الخالق محمّد أحمد ثابت الصلوي، حجيّة الخبرة الجنائيّة، دراسة مقارنة، رسالة دكتورا، كلية الدراسات العليا، أكاديمية الشرطة، 2008، ص 271.

الفرع الأول

قيد مشروعيّة طريقة الحصول على الدليل الالكتروني

تخضع قواعد الإثبات الجنائي لمبدأ المشروعيّة ومقتضاه أنّ الدليل الجنائي بما يتضمّنه من أدلة مستخرجة من وسائل إلكترونيّة كالكمبيوتر مثلا، لا يكون مشروعا ومن ثمّ مقبولا في الإثبات، إلاّ إذا جرت عملية البحث عنه والحصول عليه وإقامته أمام القضاء في إطار أحكام القانون واحترام قيم العدالة وأخلاقياتها التي يحرص على حمايتها[1]، فإذا كان المشرع يلقي على كاهل المحقق مهمة كشف الحقيقة في شأن الجريمة وجمع أدلتها فإنّ عمله مشروط بأن يتمّ في رحاب الشرعيّة، وذلك باحترام حقوق الأفراد وعدم المساس بها إلا في الحدود التي يقررها القانون، فإن تجاوز المحقق هذه الحدود وتمكّن من الحصول على دليل يثبت وقوع الجريمة، وجب طرح هذا الدليل وعدم قبوله في الإثبات[2].

ولقد وضعت الاتفاقيات الدوليّة[3]، والدساتير الوطنيّة[4] والقوانين الإجرائيّة المختلفة[5] نصوصا تتضمّن ضوابط لشرعيّة الإجراءات الماسة بالحريّة ومن ثمّ فإنّ مخالفة هذه النصوص في تحصيل الدليل الجنائي يصمّ هذا الدليل الجنائي بعدم المشروعيّة، ومن هنا فإنه لا يجوز للقاضي أن يقبل في إثبات إدانة المتهم دليلا الكترونيا تمّ حصوله من تفتيش لنظام معلوماتي باطل، وذلك إثر صدور إذن من جهة غير مختصّة، أو لم تكن الجريمة الالكترونية محل الإذن قد وقعت بعد .. .

غير أنّ ذلك لا يعني حصر حالات عدم المشروعيّة في نطاق مخالفة النصوص المقرّرة لضمانات الحريّة الفرديّة، إذ بعيدا عن هذه النصوص يصمّ الفقه والقضاء الدليل بعدم المشروعيّة متى كانت طريقة الحصول عليه تتعارض مع القواعد العامة للإجراءات الجنائيّة

---

(1) Djavad (F)، le fardeau de la preuve en matière pénale essai d'une théorie générale، thèse Paris، 1977، p. 26.

(2) وفي ذلك تقرر محكمة النقض بأنّه لا يجوز إدانة المتهم إلى دليل ناشئ عن إجراء باطل (نقض 2/1/1990) مجموعة أحكام النقض س 40 رقم 2 ص 27).

(3) راجع على سبيل المثال المواد:(5 ــ 11ــ 12)من الإعلان العالمي لحقوق الإنسان لسنة 1948. والمواد (3 ــ 8ــ 38) من الاتفاقية الأوربيّة لحقوق الإنسان والحريات الأساسيّة لسنة 1950. وكذلك الاتفاقيّة الدوليّة ضد التعذيب وسائر المعاملات غير الإنسانيّة والحاطة من الكرامة البشريّة لسنة 1984. وأيضا الاتفاقيّة الأوربيّة لمنع التعذيب والمعاملة غير الإنسانيّة أو المهينة لسنة 1987.

(4) راجع المواد:(17ــ 19ــ 27ــ 41ــ 42ــ 44ــ 45ــ 71) من الدستور المصري لسنة 1971. وأيضا المواد: (46ــ 48ــ 32ــ 34 فقرة 2ــ 35) من الدستور الجزائري لسنة 1996.

(5) راجع المواد:(34ــ 35ــ 91ــ 94 ــ 95ــ 141ــ 206) من قانون الإجراءات الجنائيّة المصري. كذلك المادتين (41 و 44)من قانون الإجراءات الجزائيّة الجزائري.

والمبادئ القانونيّة العامة[1]، كالقواعد والمبادئ التي توجب "احترام قيم العدالة وأخلاقياتها[2]" و"النزاهة في الحصول على الأدلة" و"احترام حقوق الدفاع"[3][4].

والواقع أنّ هذا القيد يمثّل المقابل لحريّة القاضي الجنائي في قبول جميع أدلة الإثبات، بما فيها تلك التي لم ينظمها المشرع، فالمعروف أنّ القانون قد اقتصر على الإشارة على بعض أهم وسائل الإثبات وأكثرها شيوعا في العمل، وترك الباب مفتوحا أمام ما قد يستجد من وسائل أخرى، يكون من شأنها تيسير الوصول إلى الحقيقة، لذلك يكون قيد المشروعية كوسيلة لفلترة وسائل الإثبات الجنائي، هذا من جهة.

ومن جهة أخرى يكتسب هذا القيد أهميّة كبرى نتيجة التقدم الهائل الذي تحقّق في السنوات الأخيرة في شأن الوسائل الفنيّة للبحث والتحقيق والتي تسمح أكثر فأكثر باختراق مجال الحياة الخاصة للأفراد، وإن كان في مقابل ذلك يرضي أو يلبي مقتضيات العدالة الجنائيّة على مكافحة الجريمة بصفة عامة والجريمة الالكترونيّة بصفة خاصة.

وممّا يثار بحثه في هذا الصدد مسألتان: الأولى، مدى إمكانيّة قبول دليل الكتروني غير مشروع وذلك حماية للمصلحة العامة على حساب المصلحة الخاصة للأفراد. والمسألة الثانيّة: تتمثل في قيمة الدليل غير المشروع في الإثبات الجنائي، وهل يجوز قبول الدليل الالكتروني غير المشروع في حالة البراءة. وهل يستوي الأمر في ذلك عند مختلف النظم القانونيّة .

وعلى ذلك، سوف نجيب على هذه الإشكاليات من خلال النقاط التالية:

أوّلا ـ مشكلة المصلحة الأولى بالرعاية: وهي الحالة التي يكون فيها دليل الالكتروني غير المشروع كأثر للتعدّي على الحياة الخاصة من جهة، وفي نفس الوقت يعدّ وسيلة إثبات لجرائم تهدّد أمن ونظام المجتمع الأخلاقي، فأي المصلحتين أولى بالرعاية.

---

(1) قضت محكمة النقض البلجيكيّة بأن وصف الدليل غير المشروع لا يقتصر فقط على الفعل الذي يحظره القانون صراحة بل يشمل كل فعل يتعارض مع القواعد الجوهريّة للإجراءات الجنائيّة أو المبادئ القانونيّة العامة. انظر: د/ جميل عبد الباقي الصغير، أدلة الإثبات الجنائي والتكنولوجيا الحديثة، المرجع السابق، ص 110.

(2) د/ محمد زكي أبو عامر، المرجع السابق، ص 120.

(3) د/ ياسر الأمير فاروق محمد، المرجع السابق، ص 626.

(4) وانطلاقا من ذلك تختلف قاعدة مشروعيّة الدليل الجنائي عن قاعدة شرعيّة الجرائم والعقوبات، حيث تعني هذه الأخيرة مجرد التوافق مع أحكام القاعدة القانونيّة المكتوبة، بخلاف القاعدة الأولى فهي أعم، حيث تشمل فضلا عن القواعد القانونيّة، المبادئ التي نصت عليها المواثيق والمعاهدات الدولية وقواعد النظام العام وحسن الآداب السائدة في المجتمع، بالإضافة إلى المبادئ التي استقرت عليها محكمة النقض، وبذلك توفر قاعدة مشروعيّة الدليل حماية كافية لحماية حريّة الإنسان، إذا ما اتخذت ضده إجراءات ماسة بحريّته من غير الطريق القانوني.

فإذا كان البعض يشكّ في مشروعية الدليل الالكتروني، باعتباره طريقة للتدخل في الحياة الخاصة للأفراد، لاسيما في مجال الجرائم الجنسية، حيث يكون السلوك الجنسي برضاء المشتركين فيه. إلاّ أنّنا نرى أنّ الاستعانة بالوسائل العلمية الحديثة مثل الانترنت، واستخدامه كدليل على وقوع جريمة الإعلان عن البغاء ونشر المطبوعات الفاضحة يستهدف المصلحة العامة، وحتى تتمكن الدولة من حماية النظام الاجتماعي حتى لا ينهار هذا النظام بسبب احترام مبالغ فيه للحقوق والحريات الخاصة ولا يمكن الاعتراض عليه بحجة عدم مشروعيّة الدليل الالكتروني، فكل ما يسفر عنه العلم الحديث يجب أن يستخدم في تحقيق أمن المجتمع ولا شك في مشروعيته.

وإذا تمّ التسليم بالقول بأنّ هناك تعدّ على حريات الأفراد فإنّه تعدّ ضئيل للغاية، ومما يتعيّن الاعتداد به هو مدى خطورة العدوان أو المساس بالنظام الاجتماعي، فلا يمكن استبعاد كل وسيلة لمجرد منافاتها للقواعد العامة دون دراسة أو تعمق لآثارها على المجتمع.

ثانيا ـ قيمة الدليل غير المشروع: سوف نتناوله من وجهة نظر النظام اللاتيني والأنجوأمريكي وفي ذلك نوع من التفصيل فيما يلي:

أ ـ قيمة الدليل غير المشروع في النظام اللاتيني: نميز في ذلك بين نوعين من الأدلة، دليل الإدانة ودليل البراءة.

- **بالنسبة لدليل الإدانة:** انطلاقا من قاعدة أنّ الأصل في الإنسان البراءة فإنّ المتهم يجب أن يعامل على أساس أنّه بريء في مختلف مراحل الدعوى إلى أن يصدر بحقّه حكم بات(نهائي)، وهذا يقتضي أن تكون الأدلة التي يؤسّس عليها حكم الإدانة مشروعة سواء كانت أدلة تقليدية أو ناتجة عن الوسائل الالكترونيّة بصفة عامة، ومن أمثلة الطرق غير المشروعة التّي يمكن أن تستخدم في الحصول على الدليل الالكتروني، إكراه المتهم المعلوماتي من أجل فك شفرة الدخول إلى النظم المعلوماتيّة، أو كلمة السر اللازمة للدخول إلى ملفات البيانات المختزنة، وتتسم بعدم المشروعيّة أيضا أعمال التحريض على ارتكاب الجريمة الالكترونيّة من قبل رجال الضبط القضائي، كالتجسّس المعلوماتي أو المراقبة الالكترونيّة عن بعد دون مسوّغ قانوني.

وانطلاقا من ذلك فأيّ دليل يتمّ الحصول عليه بطريقة غير مشروعة يتمّ إبطاله بما في ذلك الدليل الالكتروني[1]، وعدم إنتاج الإجراء الباطل للآثار التّي تترتّب عليه مباشرة، حيث

---

[1] وفي ذلك أوصى المؤتمر الدولي الخامسّ عشر للجمعيّة الدوليّة لقانون العقوبات، والذي عقد في ريودي جانيرو بالبرازيل في الفترة من 4ـ 9 سبتمبر سنة 1994 في مجال حركة إصلاح الإجراءات الجنائيّة وحماية حقوق الإنسان بمجموعة من التوصيات، منها التوصيّة رقم (18) التي تنص على أنّ كل الأدلة==

حدّدت المادة (336) من قانون الإجراءات الجنائيّة المصري ذلك فنصّت على أنّه" إذا تقرّر بطلان أي إجراء، فإنّه يتناول جميع الآثار التي تترتب عليه مباشرة، ويلزم إعادته متى أمكن ذلك". وهي نفس القاعدة المتبعة في قانون الإجراءات الجزائيّة الجزائري، حيث نصّت المادة (157 فقرة 1) من ذات القانون على أن " تراعى الأحكام المقرّرة في المادة المتعلقة باستجواب المتهمين والمادة (105) المتعلقة بسماع المدعي المدني وإلاّ ترتب على مخالفتها بطلان الإجراء نفسه وما يتلوه إجراءات ..". ونصّت المادة (191) من قانون الإجراءات الجزائيّة الجزائري على أن " تنظر غرفة الاتهام في صحّة الإجراءات المرفوعة إليها وإذا تكشّف لها سبب من أسباب البطلان قضت ببطلان الإجراء المشوب به وعند الاقتضاء ببطلان الإجراءات التالية له كلها أو بعضها..".

وإذا كانت القاعدة أنّ الإجراء الباطل يمتدّ بطلانه إلى الإجراء والإجراءات اللاحقة له مباشرة، غير أنّ هذه القاعدة تثير مسألة في غاية الأهميّة تتعلّق بماهية المعيار الذي يبيّن مدى العلاقة التي تربط بين العمل الإجرائي والأعمال التالية له حتى يمتدّ إليها البطلان. وقد تعدّدت المعايير التي قال بها الفقه المقارن[1]، والمعيار الراجح والسائد في مصر والجزائر هو أنّ العمل اللاحق يعتبر مرتبطا بالإجراء السابق إذا كان هذا الأخير مقدمة ضروريّة لصحة العمل اللاحق، فإذا أوجب القانون مباشرة إجراء معيّن قبل آخر بحيث يصبح الأول بمثابة السبب الوحيد للإجراء الذي تلاه كان الإجراء الأول شرطا لصحة الإجراء التالي له، فإذا بطل ترتب عليه بطلان الإجراء الذي بني عليه[2] .

- **بالنسبة لدليل البراءة:** هناك اختلاف حول مدى اشتراط المشروعيّة بوجه عام في دليل البراءة ويمكن ردّ هذا الخلاف إلى اتجاهات ثلاثة، الأوّل: يتمسّك باعتبار المشروعيّة شرطا لازما في كل دليل والاتجاه الثاني: يقصر المشروعيّة على دليل الإدانة وحده وهو

==التي يتمّ الحصول عليها عن طريق انتهاك حق أساسي للمتهم والأدلة الناتجة عنها تكون باطلة، ولا يمكن التمسك بها أو مراعاتها، في أيّ مرحلة من مراحل الإجراءات، وقد أشار هذا المؤتمر إلى ضرورة احترام مبدأ المشروعية عند البحث عن الدليل في جرائم الحاسب الآلي والجرائم التقليدية في بيئة تكنولوجيا المعلومات، وإلاّ ترتب عليه بطلان الإجراء فضلا عن تقرير المسؤوليّة الجنائيّة لرجل السلطة العامة الذي انتهك القانون. لمزيد من التفصيل حول هذا المؤتمر انظر:

- XV(15ème) Congrès International de droit pénal، Rio de Janeiro، Brésil، 4-9 septembre 1994، Association Internationale de droit pénale، R. I. D.P، 1er et 2eme trimestres 1995، p.38.

[1] د/ أحمد فتحي سرور، نظريّة البطلان في قانون الإجراءات الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1959، ص 182.

[2] د/ أحمد فتحي سرور، نفس المرجع ، ص 382 وما بعدها.

ما تأخذ به محكمة النقض، والاتجاه الثالث: يذهب إلى التفرقة بين ما إذا كانت طريقة الحصول على الدليل غير المشروع ترقى إلى مرتبة الجريمة من عدمه.

- **الاتجاه الأول**[1]: يرى أنّ المشروعيّة لازمة في كل دليل سواء أكان إدانة أو براءة، وذلك تأسيسا على نص المادة (336) من قانون الإجراءات الجنائية المصري التي تقرر بطلان جميع الآثار المترتبة على الإجراء الباطل دون تفرقة بين دليل إدانة ودليل براءة، أضف إلى أنّ قصر المشروعية على دليل الإدانة فقط دون البراءة فيه وبالا على الفرد والمجتمع، لأنّه يؤدي إلى اعتبار التزوير وشهادة الزور وإرهاب الشهود حتى يعدلوا عن أقوالهم مشروعة لإثبات البراءة، وينتهي هذا الاتجاه إلى أن إثبات البراءة ــ كالإدانة ــ لا يكون إلا من خلال سبل مشروعة ولا يصح أن يتلف إثبات البراءة من قيد المشروعية الذي هو شرط أساسي في أيّ تشريع لكل اقتناع سليم.

ــ **الاتجاه الثاني**[2]: يرى أنّ المشروعية لازمة في دليل الإدانة دون البراءة تأسيسا على أنّ المحكمة لا تحتاج إلى اليقين في إثبات البراءة بل يكفي في ذلك الشك وهو ما يمكن الوصول إليه من خلال أي دليل ولو كان غير مشروع، أضف إلى ذلك أنّ للمتهم الحريّة الكاملة في اختيار وسائل دفاعه بقدر ما يسعفه مركزه في الدعوى وما تحيط نفسه من عوامل الخوف والحذر وغيرها من العوارض الطبيعيّة لضعف النفوس البشريّة والإصرار على تطلب مشروعيّة دليل البراءة أسوة بدليل الإدانة يعرقل حق المتهم في الدفاع عن نفسه الذي يعلوا على حق المجتمع في استيفاء العقاب.

وتعتنق محكمة النقض هذا الاتجاه وقد عبّرت عنه بقولها :"إن كان يشترط في دليل الإدانة أن يكون مشروعا إذ لا يجوز أن تبنى إدانة صحيحة على دليل باطل في القانون، إلاّ أنّ المشروعيّة ليست بشرط واجب في دليل البراءة ، ذلك أنّه من المبادئ الأساسيّة في الإجراءات الجنائيّة أنّ كل متهم يتمتع بقرينة البراءة حتى يحكم بإدانته نهائيّا"[3]

---

[1] انظر في هذا الاتجاه: د/ رؤوف عبيد، مبادئ الإجراءات الجنائيّة في القانون المصري، المرجع السابق، ص 740. د/ محمود نجيب حسني، المرجع السابق، ص 437 هامش رقم (2) .

[2] انظر في هذا الاتجاه محمود محمود مصطفى، شرح قانون الإجراءات الجنائيّة، المرجع السابق، ص 424، د/ أحمد فتحي سرور ، المرجع السابق، ص 752. وانظر أيضا د/ مأمون سلامة، ، المرجع السابق، ص 174. د/ محمد زكي أبو عامر، المرجع السابق، ص 117 هامش رقم (35). د/ هلالي عبد الله أحمد، النظرية العامة للإثبات الجنائيّ، المرجع السابق، ص 584.

[3] نقض 31 يناير 1967، مجموعة أحكام النقض، س 18، رقم 24، ص 128. نقض 15 فبراير سنة 1984، مجموعة أحكام النقض، س 35، رقم 31 ، ص 153.

ـ **الاتجاه الثالث**[1]: ويرى ضرورة التفرقة بين ما إذا كان دليل براءة قد تمّ الحصول عليه نتيجة سلوك يعدّ جريمة جنائيّة وما إذا كان قد تمّ الحصول عليه نتيجة سلوك يشكل مخالفة لقاعدة إجرائيّة، فإن كان الأول وجب إهدار الدليل وعدم الاعتداد به، لأنّ القول بغير ذلك مفاده استثناء بعض الجرائم من العقاب، والدعوى إلى ارتكابها وهو ما لا يجوز وتأباه الشرائع القويمة، أما إذا كان الحصول على الدليل يخالف قاعدة إجرائيّة فحسب فهنا يصح الاستناد إلى هذا الدليل في تبرئة المتهم تحقيقا للغاية من تشريع البطلان، ولأنّ الفرض أنّ البطلان الذي شاب وسيلة التوصل إلى الدليل إنما يرجع إلى فعل من قام بالإجراء الباطل، وبالتالي لا يصح أن يضار المتهم بسبب لا دخل له فيه.

وفي إطار الترجيح بين الاتجاهات الثلاثة نجد أنفسنا نؤيد الاتجاه الثاني والذي يقصر المشروعيّة على دليل الإدانة دون البراءة وذلك لعدّة أسباب:

1 ــ أنّ القاعدة هي افتراض البراءة في المتهم ومن تمّ فإنّ أيّ دليل يساعد على تأكيد هذه القاعدة يجب قبوله دون الالتفات لأي اعتبار آخر.

2 ــ قيد المشروعيّة ذاته وهو احترام حقوق الدفاع ممّا يستتبع قصر هذا القيد على دليل الإدانة هو وحده الذي يمسّ حق الدفاع أما قيد البراءة فلا يخضع لهذا القيد[2].

3 ــ كذلك فإنّ العدالة لا تضار إذا أفلت مجرم من العقاب استنادا إلى دليل غير مشروع، لأنّه لا يضير العدالة إفلات مجرم من العقاب بقدر ما يضيرها إدانة برئ.

ب ـ قيمة الدليل غير المشروع في النظام الأنجلوأمريكي: يختلف مضمون قاعدة مشروعيّة الدليل بما يتضمّنه من مخرجات الوسائل الالكترونيّة كالكمبيوتر مثلا ضيقا واتساعا في النظام الأنجلوأمريكيّ حسب نطاق ما يسمى بقاعدة الاستبعاد(The exclusion)، وعلى ذلك، سوف نتناول من خلال التالي نموذجين من القوانين، القانون الانجليزي والقانون الأمريكي، وان كان في الأصل ينتمان إلى نفس العائلة، إلاّ أنّ هناك فروقا بينهما فيما يتعلق مدى قبول أو استبعاد الدليل غير المشروع، سواء كان تقليديا أو مستخرجا من كمبيوتر مثلا أو أيّ وسيلة الكترونيّة وذلك من خلال دراسة كل قانون على حدة.

1 ـ بالنسبة للقانون الإنجليزي: القاعدة الأساسيّة في نظام القانون العام أنّه متى كان الدليل منتجا في الإثبات فهو مقبول، أيّا كانت الطريقة التي تمّ الحصول عليه من خلالها، أي حتّى

---

[1] انظر في هذا الاتجاه: د/ سامي حسني الحسيني، النظرية العامة للتفتيش في القانون المصري والمقارن، المرجع السابق، ص 471 وما بعدها. د/ محمد عيد الغريب، حريّة القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائيّة، النسر الذهبي للطباعة، 1996ــ 1997، ص 62.

[2] د/ ياسر الأمير فاروق محمد، المرجع السابق، ص 655.

ولو كان ذلك بطريق غير مشروع[1]، ففي قضيّة (V.Owen) وفيها قام رجل الشرطة بتفتيش المستأنف بصورة غير قانونيّة، وعثر كميّة من سمك "السالمون" في جيبه، فتمّ قبولها كدليل في قضيّة صيد بدون ترخيص وقال في ذلك القاضي(Mellor)، أنّ عدم قبول الأدلة بسبب الحصول عليها بطريقة غير مشروعة، يمثّل عائقا خطيرا لإدارة العدالة الجنائيّة.

إلاّ أنّه بعد ذلك ظهر اتجاه آخر في القضاء يخفّف من صرامة وحدّة مبدأ قبول الدليل أيّا كانت طريقة تحصيله[2]، إلاّ أنّه سرعان ما تمّ العودة إلى تكريس مبدأ الإطلاق في عدم استبعاد الدليل غير المشروع، والمضي باتجاه نظريّة الضبط الجرمي[3].

وفي سنة(1984)، صدر قانون الشرطة والإثبات الجنائيّ والذي تمّ العمل به منذ(1986) حيث جاء ليعالج اختصاص الشرطة وقواعد الإثبات الجنائي على نحو يحقق ضمانات إجرائيّة هامة تفيد منها إدارة العدالة الجنائيّة، وقد تضمّن هذا القانون أحكاما تنظم استبعاد الأدلة غير المشروعة، حيث أفرد ثلاثة مواد خاصة بهذه الأحكام هي: المادة (76) والمادة(78)، والمادة (3/82).

فجاءت المادة (76) منه منظمة لقواعد استبعاد الاعتراف الذي يتمّ إمّا : باستعمال وسيلة قسريّة ضد المتهم، أو أنّه غير حقيقي، أو لا يعتمد عليه[4] أيّ قيل أو حصل من أيّ شخص غير المتهم.

أمّا المادة (78) تنظم السلطة التقديرية للقضاة في استبعاد الدليل، حيث يجوز للمحكمة أن ترفض السماح بقبول الأدلة التي قدمها الادعاء، إذا ظهر للمحكمة من خلال تقدير كافة الظروف بما فيها الظروف التي تمّ فيها تحصيل الدليل، وأنّ قبول الأدلة يمكن أن يحدث تأثيرا مضادا على نزاهة الإجراءات إلى حدّ أنّ المحكمة تقضي بعدم قبولها.

وممّا يلاحظ أنّ هذه المادة لم تورد أيّ معايير أو ضوابط بشأن إعمال أحكام هذه المادة، وكل ما بيّنه هو ألاّ يؤثر الدليل على نزاهة الإجراءات، ولا يوجد معيار محدد يوضح متى

---

[1] د/ أحمد ضياء الدين خليل، المرجع السابق، ص 756. وانظر أيضا: د/ أحمد عوض بلال، قاعدة استبعاد الأدلة المتحصلة بطريق غير مشروع في الإجراءات الجنائيّة المقارنة، المرجع السابق، ص 41.

[2] وظهر ذلك واضحا في قول اللوردات (Goddard)، بأنّه إذا كانت الأدلة مناسبة أو ذات صلة وعلاقة بالمسألة محل البحث، لا يهم كيف تمّ الحصول عليها، وذهب إلى أبعد من ذلك، بقوله أنّ القاضي له سلطة تقديريّة أو تخييريّة في عدم قبول الدليل إذا كانت صرامة القواعد الخاصة بالقبول ستؤدي إلى نتيجة غير عادلة ضد المتهم، فإذا تمّ تحصيل بعض الوثائق من المتهم بطريق الخداع، لاستخدامها كدليل ضده، لاشك أنّ القاضي له أن يستبعدها. انظر: د/ عماد عوض عدس، التحريّات كإجراء من إجراءات البحث عن الحقيقة، دار النهضة العربيّة، القاهرة، 2007، ص 394.

[3] د/ عماد عوض عدس، نفس المرجع، ص 395.

[4] د/ أحمد عوض بلال، المرجع السابق، ص 47.

تكون الإجراءات غير عادلة أو غير نزيهة. ولذلك أوجد بعض الفقهاء معايير محددة، يمكن استلهامها أثناء تطبيق نصوص المادة (78)، تتمثل في ثلاثة مبادئ، أول مبدأ هو حسن النيّة (Good faith)[1]، وثانيه مبدأ الحماية (Protective principle) ويدور حول فكرة حماية المتهمين، وآخر مبدأ هو مبدأ المخالفة الجوهريّة (Significant breach) لنصوص قانون الشرطة والدليل الجنائي لعام 1984.

وتطبيقا لذلك، رفض القاضي في إحدى القضايا قبول تسجيلات على أساس أنّها تمّت من خلال شرك خداعي، حيث قام البوليس بتركيب جهاز التنصت على خط تلفون إحدى الشاكيات بناء على موافقتها، وقد افتعلت الشاكيّة عدّة مكالمات تلفونيّة مع الشخص محل الاشتباه، وقد تمّ تسجيل هذه المكالمات التي تضمّنت موضوعات تدين المتهم[2].

أمّا المادة (3/82) فتنظم السلطة التقديريّة للقضاة المقرّرة في قواعد النظام العام(Common Law)[3] .

2 ـ **بالنسبة للقانون الأمريكي**: كان القضاء الأمريكي في البداية يتبنى القاعدة الانجليزيّة التي سادت في نظام القانون العام ــ أي عدم استبعاد الأدلة المتحصلة بطرق غير مشروعة ــ إلى أن لاحظت المحكمة الفدراليّة العليا بطريقة عارضة عام 1886 في قضيّة (Boyd v. United States)، ضرورة حظر إدانة الفرد بأدلة مستمدة من شخصه أو مسكنه تمّ الحصول عليها دون سبب معقول أو بكيفيّة غير معقولة [4]، وذلك رغبة في حماية الفرد من تعسفات السلطة. إلاّ أنّ البداية الحقيقيّة لتكريس قاعدة استبعاد الدليل غير المشروع ترجع إلى قضيّة شهيرة عام 1914، هي قضيّة (Weeks v. United States)[5]، والتي قرّرت فيها المحكمة الاتحاديّة العليا بإجماع أعضائها مبدأ عدم قبول الدليل المتحصل بالمخالفة للتعديل الدستوري الرابع أمام المحاكم الاتحاديّة.

---

[1] وتطبيقا لهذا المبدأ، قالت محكمة الاستئناف أنّ الدليل المتحصل من فحص الكحول نتيجة لقبض باطل يجب أن يستبعد وذلك لوجود نيّة سيئة لدى رجل الشرطة. وفي قضاء آخر تمّ قبول الاعتراف المتحصل عليه من المتهم دون حضور محاميه، تأسيسا على وجود نيّة حسنة لدى البوليس. انظر: د/ عماد عوض عدس، المرجع السابق، ص 401ــ 402،

[2] Wasilk (Martin)، Computer crime and others crimes against information technology in United Kingdom، R. I.D.P، 1993، 642.

[3] لمزيد من التفصيل انظر: د/ عماد عوض عدس، المرجع السابق، ص 396.

[4] د/ أحمد ضياء الدين محمد خليل، المرجع السابق، ص 757.

[5] لمزيد من التفاصيل حول هذه القضيّة انظر: د/ أحمد عوض بلال، المرجع السابق، ص 86 وما بعدها.

إلاّ أنّه يرد على ذلك بعض الاستثناءات، فالمحكمة العليا التي نشأت قاعدة الاستبعاد في رحابها، حدّدت أربع حالات لا يتمّ فيها الاستبعاد، وأوّل هذه الحالات: توافر حسن النيّة لدى رجل الشرطة الذي يقوم بالعمل الإجرائي، ويستند في ذلك على أساس قانوني صحيح. وثاني هذه الحالات عندما تكون الصلة بين العمل الإجرائي المخالف والدليل المتحصل من ذلك الإجراء ضعيف وبسيط لدرجة أنّ شائبة الخطأ أو المخالفة لا يتمّ إدراكها. وثالث هذه الحالات عندما يتمّ الحصول على الأدلة بصورة مستقلة عن العمل الإجرائي المخالف، ورابع هذه الحالات، إذا كانت الأدلة ذاتها لا يتمّ اكتشافها إلا بارتياد السبيل القانوني الصحيح.

إذن فالتطبيق القضائي الأمريكي لقاعدة الاستبعاد أكثر وضوحا من التطبيق القضائي الانجليزي، ذلك أنّ نظريّة " فاكهة الشجرة المسمومة يجب أن لا تأكل" (The fruit of poisoned tree should not be eaten)، تجد لها مكانا وقبولا في التطبيق القضائي الأوّل دون الثاني، حيث أنّ الأصل في القضاء الأمريكي هو التطبيق المطلق للقاعدة، والاستثناء هو التطبيق التخييري لها [1].

وتأكيدا على ذلك، خصّص المشرّع الأمريكي مبحثا خاصا وهو المبحث الخامس في المرشد الفدرالي الأمريكي لتفتيش وضبط الحواسيب وصولا إلى الدليل الالكتروني، يتعلق "بعلاج انتهاكات الباب الثالث(قانون المراقبة)وقانون التسجيل والتقصي"، ويقصد به علاج بطلان الإجراءات غير المشروعة في الحصول على الدليل الالكتروني، حيث نصّ في ذلك على أنّه يجب على رجال الضبط القضائي والمدعيين العموميين سلوك مسلك أوامر الباب الثالث وقانون التسجيل والتقصي، عند التخطيط للمراقبة الالكترونيّة، إذ يمكن أن تسفر الانتهاكات عن غرامات وجزاءات مدنيّة وجزاءات جنائيّة **وبطلان الدليل الذي تمّ الحصول عليه**[2].

---

[1] وتطبيقا لذلك رفضت المحكمة العليا الأمريكية قبول دليل متحصّل من تفتيش باطل، ذلك أنّ البوليس قام بتفتيش سطح منزل السيدة (Mapp)، وضبطت مواد فاسدة بطريقة غير قانونيّة.

Mapp v. Ohio (1961) 367 us and see also Moran v. Barbire (1986).

انظر:

- Daniel E. Hall، Criminal Law and Procedure، (4) forth edition، Thompson Delmar Learning Publisher، p. 303.

- James J، Thomkoviz، Welsh S. White، Criminal Procedure : Constitutional constraints upon Investigation and proof، (4) forth edition، Lexis Nexis Publisher، p. 738.

[2] د/ عمر محمد بن يونس، الإجراءات الجنائيّة عبر الانترنت في القانون الأمريكي، المرجع السابق، ص 400.

الفرع الثاني
القيود المستمدة من نصوص قانونيّة خاصّة

إلى جانب القيد العام والسالف ذكره وهو قيد مشروعيّة الدليل الالكتروني، هناك قيود أخرى ترد على سلطة القاضي الجنائي في قبول الدليل الالكتروني، وهي محدّدة بنصوص قانونيّة خاصّة، وتنحصر في نوعين من القيود: يتمثل الأول في التقيّد بأدلة معيّنة في جريمة الزنا، أمّا الثاني فيتعلّق بطرق الإثبات الخاصة بالمواد غير الجنائيّة. وسنحاول من خلال التالي معرفة موقف الدليل الالكتروني من هذه القيود فهل تطبّق عليه هذه القيود شأنه في ذلك شأن أي دليل جنائي تقليدي، أم يستثنى من هذه القيود، وهو ما سنحاول معرفته من خلال التالي.

أوّلا- قيد تحديد الأدلة في جريمة الزنا:

أورد المشرع المصري عددا من الأدلة الجنائيّة التي تقبل وتكون حجة دون غيرها في إثبات جريمة الزنا، وذلك على سبيل الحصر لا المثال، حيث تنص المادة (276) من قانون العقوبات المصري على أنّ الأدلة التي تقبل وتكون حجة على المتهم بالزنا، هي القبض عليه حين تلبسه بالفعل أو اعترافه أو وجود مكاتيب أو أوراق أخرى صادرة منه أو وجوده في منزل مسلم في المحل المخصص للحريم[1]. والواضح من هذا النص أنّ المشرع المصري حدّد الأدلة التي تقبل في شأن إثبات الزنا وحصرها في : التلبس بالزنا، والاعتراف، ووجود أوراق صادرة من المتهم، ووجوده في المنزل المخصص للحريم ، وبذلك يكفي توافر أحد هذه الأدلة لإمكان الحكم على المتهم بالزنا.

أما بالنسبة للمشرع الجزائري اقتصر على ثلاثة أنواع من هذه الأدلة فحسب لإثبات جريمة الزنا وذلك ما نصت عليه صراحة المادة (341) من قانون العقوبات الجزائري، على أنّ الدليل الذي يقبل عن ارتكاب الجريمة المعاقب عليها بالمادة(339) يقوم إمّا على محضر قضائي يحرّره أحد رجال الضبط القضائي عن حالة التلبس ، وإما بإقرار وارد في رسائل أو مستندات صادرة من المتهم وإمّا بإقرار قضائي[2].

---

[1] هذا النص منقول عن المادة(338) من قانون العقوبات الفرنسي، وقد ألغيت هذه المادة بمقتضى قانون 11 جويلية 1975، حيث كانت تنص على الأدلة التي تقبل وتكون حجة على شريك الزوجة الزانيّة هي التلبس بالجريمة، أو وجود خطابات ومكاتيب صادرة عن المتهم. انظر: Roger Merle et André Vitu ،op cit، p. 167.

[2] أكّدت المحكمة العليا الجزائريّة أنّ جريمة الزنا المعاقب عليها في المادة (339) من قانون العقوبات لا تثبت إلاّ بالطرق التي أوردها المشرع على سبيل الحصر في المادة (341) من نفس القانون، وأنّ قضاة الموضوع عندما أدانوا المتهمين بجريمة الزنا على قرائن لم تنص عليها المادة(341) من قانون العقوبات==

ويذهب الراي الغالب في القضاء[1] والفقه[2] المصري إلى أنّ الأدلة سالفة البيان لازمة فقط لإثبات زنا شريك الزوجة الزانيّة أما بالنسبة للزوجة أو للزوج أو شريكته، فإثبات الزنا على أيّ منهم يخضع لمبدأ حريّة الإثبات الجنائي[3].

ولهذا لا يجوز للقاضي الجنائي أن يقبل لإثبات الزنا في حق شريك الزوجة أدلة أخرى غير ما قرّره نص المادة(276) عقوبات مصري. ولو كان دليلا الكترونيّا، سواء كان عبارة عن صور فيديو أو رسالة مرسلة من الشريك إلى الزوجة أو إلى غيرها عن طريق الهاتف المحمول (SMS) أو عن طريق الانترنت (E-mail) سواء تضمّنت هذه الرسالة اعترافا صريحا أو ضمنيا من الشريك بوقوع الزنا، أو فيها نوع من الكلام الذي يوحي بممارسة علاقة غير شرعية مع الزوجة [4].

وعلى ذلك، ومن أجل سدّ الفراغ التشريعي الواقع في أغلب التشريعات المعاصرة، نقوم بقياس الكتابة الالكترونيّة على المكاتيب والأوراق، خاصّة وأنّ المشرعين الجزائري

== فإنهم بقضائهم كما فعلوا قد خرقوا القانون. قرار صادر بتاريخ 02/ 07/ 1989ملف رقم 59100. انظر: المجلة القضائيّة ، عدد ثالث، 1991، ص 112.

[1] نقض11 /3/ 1984، مجموعة أحكام ا النقض، س 37 رقم 85، ص 258. نقض 13 /2/ 1976،س 37 رقم 934، ص 1227. نقض 1986/4/9، س 37 رقم 95، ص471. نقض6/11/ 1995، س 36 رقم 173، ص 1156.

[2] د/ محمود محمود مصطفى، الإجراءات الجنائيّة، المرجع السابق، ص 428. د/ عوض محمد عوض، المرجع السابق'، ص 669. د/ محمود نجيب حسني، الإجراءات الجنائيّة، المرجع السابق، ص 800. د/ أمال عثمان، المرجع السابق، ص 674.

[3] على أنّ في الفقه من يذهب إلى انصراف حكم المادة 276 عقوبات إلى كل متهم بالزنا لأنّ القانون صريح في ذلك ولا اجتهاد مع صراحة النص خصوصا فيما يسئ إلى المتهم. د/ رؤوف عبيد، مبادئ الإجراءات الجنائيّة في القانون المصري المرجع السابق، ص 742ـــ 743. ونعتقد أنّ قصر الأدلة على شريك الزوجة الزانيّة يؤدي إلى نتيجة شاذة وذلك عندما يقتنع القاضي من شهادة الشهود والقرائن بنسبة الزنا إلى الزوجة، فيقضي بإدانتها ويجد نفسه في ذات الوقت مضطرا إلى تبرئة شريكها لعدم توافر دليل من الأدلة التي يتطلّبها القانون لإثبات الزنا عليه.

[4] حاليا تمّ عرض قضيّة على القضاء المصري، حيث رفع الزوج جنحة زنا الزوجة عن طريق بلاغ إلي النيابة العامة من خلال الدكتورة ملكة يوسف المستشارة الشرعية والقانونية للأحوال الشخصية بمصر والدول العربية، لكن النيابة لم تلتفت إلي هذا البلاغ رغم أن المهندس تقدم للنيابة بمستنداته التي كانت عبارة عن أسطوانة C.D'' فرغ عليها كل ما كان يدور بين زوجته والعشيق واحتوت الأسطوانة علي اسم هذا الرجل والتفاصيل بالصوت والصورة عند إجراء مقابلات بين الاثنين عبر الانترنت وكأنهما زوجين حقيقة، إلا أن النيابة طلبت أولا تحرير محضر بالواقعة في قسم الشرطة، وذهبت الدكتورة ملكة يوسف إلي **مباحث الانترنت** لتعرض عليهم البلاغ ويجري الآن إثبات الواقعة. لمزيد من التفاصيل حول هذه القضيّة يرجى العودة إلى الموقع التالي:

http://samirbensaad.maktoobblog.com

والمصري وسّعا في تعريف الكتابة حيث نصّ المشرع الجزائري في المادة (323 مكرّر) من القانون المدني على" ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أيّة علامات أو رموز ذات معنى مفهوم مهما كانت الوسيلة التي تتضمّنها وكذا طرق إرسالها". بل أكثر من ذلك فقد ساو بين الكتابة في الشكل الالكتروني والكتابة على الورق وذلك بشرط إمكانيّة التأكد من هويّة الشخص الذي أصدرها بالكتابة الالكترونيّة (مادة 323 مكرر 2 من القانون المدني الجزائري)، خاصة وأنّ القانون لم يشترط في المكاتيب والأوراق التي تكون دليلا على فعل الزنا أن تكون موقّعة من المتّهم، طالما كان من الثابت صدورها منه[1]، وتبقى للقاضي في الأخير السلطة التقديريّة في تقدير قيمة هذه المكاتيب والأوراق مهما تجسّدت في أيّ صورة، وينبغي على القاضي في هذه الحالة أن تكون له ثقافة معلوماتية واسعة حتى يستطيع دراسة هذا النوع المستحدث من الأدلة، لاسيما أنه قابل للتعديل وبإمكان أي شخص أن يتقمّص شخصيّة معيّنة وذلك للإضرار بالشريك أو غيره وفك أواصل الأسرة .

ولذلك فإنّه كان من الأجدر بالمشرعين الجزائري والمصري أن ينصا على الدليل الالكتروني ضمن أدلة إثبات الزنا. وذلك سدّا للفراغ التشريعي الذي أصبح جليّا في أغلب التشريعات خاصّة العربية منها.

ثانيّا ـ قيد إثبات المسائل غير الجنائيّة :

من المسلم به، أنّ إثبات المسائل غير الجنائيّة التي تطرح على المحكمة الجنائيّة ويكون الفصل فيها مقدّمة ضروريّة للفصل في الدعوى الجنائيّة، يخضع للقانون الخاص بتلك المسائل (المسائل الأوليّة) سواء كانت مدنيّة أو تجاريّة أو أحوال شخصيّة، وهو ما نصّت عليه صراحة المادة(225) من قانون الإجراءات الجنائيّة المصري: "تتبع المحاكم الجنائيّة في المسائل غير الجنائيّة التي تفصل فيها تبعا للدعوى الجنائيّة طرق الإثبات المقرّرة في القانون الخاص بتلك المسائل". ويعدّ هذا النص تطبيقا لقاعدة أنّ " قواعد الإثبات إنّما ترتبط بالموضوع التي ترد عليه لا بنوع المحكمة".

غير أنّ تقييد القاضي الجنائي بوسائل الإثبات المقرّرة في القوانين غير الجنائيّة بالنسبة للمسائل الأوليّة، مشروط بأن تكون هذه المسألة عنصر مفترض في الجريمة سابقة في

---

[1] وفي ذلك قضت محكمة النقض بأنّ: القانون إذ جعل المكاتيب من الأدلة التي تقبل وتكون حجة على المتهم بالزنا لم يستوجب أن تكون هذه المكاتب موقعة من المتهم، بل كل ما استوجبه هو ثبوت صدورها منه، وإذن فلا تثريب على المحكمة إذا هي استندت في إثبات الزنا على المتهم إلى مسودات مكاتيب بينه وبين المتهمة ولو كانت غير موقعة، مادام قد ثبت صدورها عنه. نقض 28 أكتوبر سنة 1946، مجموعة القواعد القانونيّة، الجزء السابع، رقم 215، ص 195

وجودها على ارتكاب الفعل الإجرامي بمعنى ألاّ تكون هذه المسألة هي ذاتها الفعل الإجرامي وإلاّ جاز إثباتها بكافة طرق الإثبات بما فيها الدليل الالكتروني باعتبارها مسألة جنائيّة.

والمثال الواضح لذلك هو إثبات جريمة خيانة الأمانة(Abus de confiance)، فهذه الجريمة تفترض وجود عقد أمانة بين الجاني والمجني عليه سواء كان عقد الوكالة أو العارية أو الإجارة ...، وهذا العقد مسألة مدنيّة وسابق على وجود فعل الاختلاس أو التبديد الذي تقوم به الجريمة[1]. إذن فلتوقيع العقوبة على جنحة خيانة الأمانة يجب إثبات وجود أحد هذه العقود الخاصة التي تقوم عليها هذه الجنحة، وبالتالي فالقاضي الجنائي يلجأ بالضرورة إلى بحث مسبق حول قيام هذا العقد وأنّ عليه إثبات ذلك لما تمليه قواعد الإثبات في القانون المدني[2]. وعلى ذلك إذا زادت قيمة التصرف القانوني نصابا محددا (ألف جنيه بالنسبة للقانون المصري(المادة 60 من قانون الإثبات رقم (25 لسنة 1968) تمّ تعديلها بالقانون رقم (76 لسنة 2007) الصادر بتاريخ (6/ 6/ 2007)، ليتضاعف النصاب **من 500 جنيه إلى 1000 جنيها**)[3] [4]، و100،000 دينار جزائري بالنسبة للقانون الجزائري (المادة 333 من القانون المدني الجزائري) أو كان هذا التصرف غير محدّد القيمة يلزم إثباته بالكتابة.

والإشكال الذي ينبغي طرحه في هذا المقام هو: **هل يجوز للقاضي الجنائي أن يلجأ للدليل الالكتروني لإثبات العقد الخاص بالأمانة سواء كان عقد وكالة أو عارية أو غيره من العقود؟**

يمكن تمثيل هذه الصورة في حالة ما إذا قام طرفا عقد الأمانة إبرام هذا العقد عن طريق الانترنت، وكان العقد يتجسد في شكل سند أو محرّر الكتروني.

---

(1) د/ محمود نجيب حسني، المرجع السابق، ص 431.

(2) نقض 15/ 3/ 1956 مجموعة أحكام النقض، س 7 رقم 102، ص 340. نقض 17/ 3/ 1967، س 18 رقم 82، ص 436. نقض 27/ 12/ 1990، س 41 رقم 20، ص 1114.

(3) تنص المادة (60) من قانون الإثبات المصري ما يلي:" في غير المواد التجارية إذا كان التصرف القانوني تزيد قيمته **على ألف جنيه** أو كان غير محدد القيمة فلا تجوز شهادة الشهود في إثبات وجوده أو انقضائه ما لم يوجد اتفاق أو نص يقضي بغير ذلك. ويقدر الالتزام باعتبار قيمته وقت صدور التصرف ويجوز الإثبات بشهادة الشهود إذا كانت زيادة الالتزام **على ألف جنيه** لم تأت الأمن ضم الفوائد والملحقات إلى الأصل. ..".

(4) وتطبيقا لذلك قضت محكمة النقض بأنّ:" إثبات وجود عقد الأمانة في جريمة خيانة الأمانة يتعيّن الالتزام فيه بقواعد الإثبات المذكورة في القانون المدني، أما واقعة الاختلاس، أي التصرف الذي يأتيه الجاني ويشهد على أنّه حوّل حيازته من حيازة ناقصة إلى حيازة كاملة، أو نفي هذا الاختلاس ويدخل فيه رد الشيء موضوع الأمانة فإنها واقعة ماديّة يجوز إثباتها بكافة طرق الإثبات بما فيها البيّنة رجوعا إلى الأصل وهو مبدأ حريّة اقتناع القاضي الجنائي. نقض1975/1/19 مجموعة أحكام النقض، س 26، رقم 15، ص 65. المحكمة العليا الجزائريّة، غرفة الجنائيّة، 11 جانفي 1983،المجلة القضائيّة، ص 327.

وعلى ذلك، إذا كان يتعيّن على القاضي الجنائي حسب الأصل أن يستبعد الدليل الجنائي بما في ذلك الدليل الالكتروني عند إثبات المسائل الأوليّة والتقيد بما هو وارد في النصوص الخاصة بتلك المسائل، إلا أنه في هذه الحالة يستثنى منها الدليل الالكتروني، بحيث أصبح له دور جدّ مهم خاصة في المعاملات المدنيّة والتجاريّة، وذلك نتيجة دخول العالم في مجال تكنولوجيا المعلومات، وقيام ثورة علمية عالمية في مجال نقل المعلومات وتبادلها عبر الأنظمة الالكترونية، وأهمها الانترنت، حيث أدى ذلك إلى تغير مفهوم الإثبات تبعاً لإمكانية إنشاء الحقوق والالتزامات بطرق إلكترونية، والاستغناء في غالبية الأحيان عن الكتابة الورقية.

ولم يعد بالإمكان سوى الاعتراف بهذا العالم الجديد الذي يقوم على علم المعلوماتية والتكنولوجيا، وهو يعتمد أسلوباً غير ورقي، مرئياً ومنقولاً عبر الشاشة الالكترونية . وقد تمّ استبدال الملفات الورقية والمخطوطات بالأسطوانات الممغنطة والسندات الرقمية المحفوظة على أسطوانات ضوئية رقمية أو على أقراص ممغنطة، وهي تنتقل من مكان إلى آخر بسهولة وسرعة خارقة من دون أية حاجة للورق.

نتيجة لذلك، وحتى تواكب مختلف الدول هذه التطورات في مجال تكنولوجيا الاتصالات عن بعد وبالتالي تنميّة وتشجيع التجارة الالكترونيّة قامت بتوسيع تعريف الكتابة لتشمل في طياتها المحرّرات الالكترونيّة، وذلك كالتشريع الفرنسي، الجزائري والمصري، كما تمّ الاعتراف بالمحرر الالكتروني كدليل لإثبات المعاملات الإلكترونية.

وقد عرّفت المادة(1316) من القانون المدني الفرنسي **الدليل الكتابي** على أنّه " ينتج من تتابع حروف أو خصائص مطبوعة أو أرقام أو كل إشارة أو رموز لها معنى مفهوم أيًا كانت الدعامة المدون عليها ووسيلة نقله"[1]. وهو نفس التعريف الذي أخذه كل من المشرع الجزائري[2] ـــ وذلك بموجب قانون رقم (05ـــ10) المؤرخ في 20 يونيو 2005 والمعدل للقانون المدني الجزائري، ـــ أمّا المشرع المصري[3] فكان بمقتضى القانون رقم(15 لسنة

---

(1) Article 1316 du C. civil، dispose que :" La preuve littérale، ou preuve par écrit، résulte d'une suite de lettres، de caractères، de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible، quels que soient leur support et leurs modalités de transmission".

(2) عرّف المشرع الجزائري الدليل الكتابي في المادة 323 مكرر من القانون المدني الجزائري ، بنصه على انه "ينتج الإثبات بالكتابة من تسلسل حروف أو أوصاف أو أرقام أو أيّة علامات أو رموز ذات معنى مفهوم، مهما كانت الوسيلة التي تتضمّنها، وكذا طرق إرسالها"

(3) عرّف الكتابة الالكترونية بموجب المادة الأولى(1) من القانون رقم 15 لسنة 2004 الخاص بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، بأنها " كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة الكترونية أو رقميّة أو ضوئيّة أو أيّة وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك".

2004)الخاص بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، الصادر في 21 أبريل سنة 2004.

وقد أقرّ المشرع الفرنسي التماثل بين الكتابة على الورق والكتابة الالكترونيّة من حيث الحجية في الإثبات، فتنص المادة(1316ـ1) من القانون المدني الفرنسي على أنّة "تقبل الكتابة في شكل الكتروني كدليل في الإثبات مثلها في ذلك مثل الكتابة على دعامة ورقيّة، مادام أنّ الشخص المنسوب إليه هذه الكتابة قد تمّ تحديده على وجه صحيح وقد تمّ إثبات هذه الكتابة والاحتفاظ بها في ظروف من شأنها أن تضمن سلامتها"[1].

وقد أخذ المشرع الجزائري حرفيّا النص السابق ذكره، حيث تنص المادة (323 مكرر 1)على أنّه يعتبر الإثبات بالكتابة في الشكل الالكتروني كالإثبات بالكتابة على الورق، بشرط إمكانيّة التأكّد من هويّة الشخص الذي أصدرها وأن تكون معدّة ومحفوظة في ظروف تضمن سلامتها.

أمّا بالنسبة للمشرع المصري فقد أكّد هو أيضا على هذه المساواة، حيث نص في المادة (15) من القانون رقم (15 لسنة 2004) الخاص بتنظيم التوقيع الالكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، بـأنّ للكتابة الالكترونيّة وللمحرّرات الالكترونيّة في نطاق المعاملات المدنيّة والتجاريّة والإداريّة، ذات الحجيّة المقرّرة للكتابة والمحررات الرسميّة والعرفيّة في أحكام قانون الإثبات في المواد المدنيّة والتجاريّة، متى استوفت الشروط المنصوص عليها في هذا القانون وفقا للضوابط الفنيّة والتقنيّة التي تحدّدها اللائحة التنفيذية لهذا القانون. بل أكثر من ذلك فإنّ القانون السابق اعتدّ بصورة المحرّر الالكتروني بنصه في المادة 16 منه على أنّ: الصورة المنسوخة على الورق من المحرر الالكتروني الرسمي حجّة على الكافة بالقدر الذي تكون فيه مطابقة لأصل هذا المحرّر، وذلك مادام المحرّر الالكتروني الرسمي والتوقيع الالكتروني موجودين على الدعامة الالكترونيّة.

وبما أنّ المحرر الالكتروني يتكوّن من عنصرين الكتابة والتوقيع، فمن غير المتصوّر أن يبقى شكل التوقيع على المحرر الالكتروني تقليديّا بخط اليد بل يجب أن يكون من نفس تقنيّة المحرّر الالكتروني بمعنى أن يكون توقيعا الكترونيا [2]، ونتيجة لذلك تبنى المشرع

---

(1) Article 1316-1 du C. civil، dispose que :" L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier، sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité".

(2) عرفت المادة الثانية (2) من القانون النموذجي للتوقيع الالكتروني" الاونيسترال، التوقيع الالكتروني بأنه بيانات في شكل إلكتروني مدرجة في رسالة بيانات أو مضافة إليها أو مرتبطة بها منطقيا، يجوز أن ==

الفرنسي فكرة التوقيع الالكتروني وذلك بموجب القانون الصادر في(13 مارس سنة 2000) [1]، وأعطى له قوة في الإثبات إذا توافر له شرطان، الأول: استعمال وسيلة موثوق فيها بحيث تضمن ربط صاحب التوقيع بمحتوى المستند الالكتروني، والثاني: أن يتوافر في المستند الالكتروني شروط سلامته المحدّدة وفقا لمرسوم المجلس الأوربي(المادة 1316 /4 من القانون المدني الفرنسي).

انطلاقا مما سبق يتضح لنا أنّ للدليل الالكتروني أهميّة بالغة في إثبات التعاملات الالكترونيّة والتي أصبحت بدورها روح الاقتصاد للعديد من الدول، ولم نشأ التوسيع فيها حتى لا نخرج عن إطار دراستنا وهو الإثبات الجنائي.

وبالتالي فإنّ الإجابة على الإشكال الخاص بمدى إمكانية القاضي الجنائي الاستعانة بالدليل الالكتروني لإثبات المسائل الأوليّة خاصة المدنيّة والتجاريّة منها، تكون بالإيجاب، وذلك أنه المشرع نظّم في مختلف الدول المقارنةّ المعاملات الإلكترونية وسبل إثباتها وأعطى للمحرّرات الالكترونيّة حجية تامة شأنها في ذلك شأن المحررات الورقيّة بشرط اشتمالها الشروط الفنيّة والتقنيّة.

== تستخدم لتعيين هوية الموقع بالنسبة إلى رسالة البيانات، ولبيان موافقة الموقع على المعلومات الواردة في رسالة البيانات". أماّ المادة الأولى من القانون المصري رقم 15 لسنة 2004 الخاص بتنظيم التوقيع الالكتروني فقد عرّفها بأنّها: "ما يوضع على محرر إلكتروني ويتخذ شكل حروف أو أرقام أو رموز أو إشارات أو غيرها ويكون له طابع منفرد يسمح بتحديد شخص الموقع ويميزه عن غيره " .

[1] لمزيد من التفاصيل حول التوقيع الالكتروني، انظر: د/ عبد الفتاح بيومي حجازي، التوقيع الالكتروني في النظم القانونيّة المقارنة، دار الفكر الجامعي، الطبعة الأولى، 2005، ص 11 وما بعدها. وانظر أيضا: د/ نادر عبد العزيز شافي، المصارف والنقود الالكترونيّة، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، طرابلس، 2007، ص 43 وما بعدها. وانظر أيضا : د/ عبد العزيز مرسي حمود، مدى حجيّة المحرّر الالكتروني في الإثبات في المسائل المدنية والتجارية في ضوء قواعد الإثبات النافدة، مجلّة البحوث القانونيّة والاقتصادية، العدد الواحد والعشرون، السنة الحادية عشر ، أبريل 2003، ص 40 وما بعدها.

المبحث الثاني
سلطة القاضي الجنائي في تقدير الدليل الالكتروني

السائد في الفقه[1] أنّ سلطة القاضي الجنائي في تقدير الدليل بما في ذلك الدليل الالكتروني يحكمه مبدأ الاقتناع القضائي وأنّ هذا المبدأ يؤدي إلى نتيجتين هما:

الأولى – حريّة القاضي في قبول الأدلة .

الثانيّة – حريّة القاضي في تقدير الأدلة .

وإن كنا نسلم مع إجماع الفقه[2] بالنتيجة الثانية دون الأولى، ذلك أنّ هذه الأخيرة مسألة قانونيّة، لا مجال لإعمال سلطة القاضي التقديرية، حيث أنّ المشرع حسم هذه المسألة بتحديده للنموذج القانوني للدليل الخاضع لتقدير القاضي، فمتى ما توافرت شروط هذا النموذج طبقا لمبدأ الشرعيّة الإجرائيّة، وجب على القاضي إخضاعه لعمليّة تقديره. أما الثانية فمسألة تتعلّق بقيمة الدليل لإثبات الحقيقة وهي مسألة موضعيّة محضة، للقاضي أن يمارس سلطته التقديرية فيها، بل هي المجال الطبيعي لهذه السلطة حيث أنها تتعلّق بقيمة الدليل في الإثبات وصولا للحقيقة.

غير أنّ مبدأ الاقتناع القضائي إذا كان يخول القاضي الجنائي حريّة واسعة في البحث عن الأدلة (الدليل الالكتروني) وتقديرها، فهي حريّة ليست مطلقة، وإنّما هي حريّة محكومة بضوابط وقيود معيّنة، الغرض منها كفالة أن تمارس تلك الحريّة في إطارها الصحيح، بما يضمن الوصول إلى الحقيقة الفعليّة في الدعوى، ودون الافتئات على الحقوق والحريّات الشخصيّة.

وعلى هدي ما تقدّم، تقتضي دراسة سلطة القاضي الجنائي في تقدير الدليل الالكتروني أن نحدّد في المطلب الأوّل حريّة القاضي الجنائي في الاقتناع بالدليل الالكتروني، أمّا في المطلب الثاني سنتناول الضوابط التي تحكم اقتناع القاضي بالدليل الالكتروني، وذلك على الوجه التالي:

---

[1] د/ محمود محمود مصطفى، الإثبات في المواد الجنائيّة في القانون المقارن، المرجع السابق، ص 95. وانظر أيضا: د/ محمود نجيب حسني، المرجع السابق، ص 438، وأنظر كذلك: د/ محمّد زكي أبو عامر، المرجع السابق، ص 127.

[2] د/ فاضل زيدان محمد، المرجع السابق، ص 93.

المطلب الأوّل

حريّة القاضي الجنائي في الاقتناع بالدليل الالكتروني

يخضع الدليل الالكتروني للمبدأ العام في الإثبات الجنائي وهو حريّة القاضي الجنائي في الاقتناع (L'intime conviction)، وحريّته في هذا المقام بالغة السعة، فهو وحده الذي يقدّر قيمة الدليل الالكتروني بحسب ما تحدثه من أثر في وجدانه من ارتياح واطمئنان، ومع ذلك

ولقد تعاظم دور الإثبات العلمي مع ظهور الدليل الالكتروني المطلوب للإثبات في الجرائم الالكترونيّة، ممّا جعل القاضي أنّه يضطر للتعامل مع هذا النوع المستحدث من الأدلة الضرورية لكشف أنماط جديدة من الجرائم في مقابل نقص الثقافة المعلوماتية، وممّا يزيد من نسبة هذا الاضطرار المشكلات التي يثيرها هذا الدليل، ممّا تؤدي إلى إنقاص قيمته ونسبة الاستناد عليه في إثبات الجرائم الالكترونيّة.

وعلى ذلك، سنتناول في الفرع الأوّل، الطبيعة العلمية للدليل الالكتروني وأثرها على اقتناع القاضي الجنائي، ثمّ مشكلات الدليل الالكتروني ومدى تأثيرها على اقتناع القاضي الجنائي، وذلك في الفرع الثاني.

الفرع الأول

الطبيعة العلمية للدليل الالكتروني وأثرها على اقتناع القاضي

يقتضي الحديث عن الطبيعة العلميّة للدليل الالكتروني وأثرها على اقتناع القاضي الجنائي، بيان مضمون مبدأ الاقتناع القضائي وما يعنيه في مجال الإثبات الجنائي، ثمّ بيان قيمة الدليل الالكتروني في الإثبات الجنائي، ومادام أنّ الدليل الالكتروني يعدّ تطبيقا من تطبيقات الدليل العلمي، يتعيّن علينا أن نتاوله بالدراسة بالإضافة إلى مدى تأثّر القاضي الجنائي به، فهل يسلم ويبني اقتناعه بالدليل الالكتروني على أساس أنّ أمره محسوم علميّا، ذلك ما سيتمّ تناوله في التالي على النحو الآتي:

أوّلا- مفهوم مبدأ الاقتناع القضائي:

يعدّ مبدأ الاقتناع القضائي أحد أهم المبادئ التي تقوم عليها نظريّة الإثبات في المواد الجنائيّة، وعنه تتفرّع معظم القواعد التي تحكم هذا الإثبات[1]. وعلى ذلك، سوف نوضح في البداية التعريف بهذا المبدأ ونبيّن الأساس القانوني الذي يقوم عليه في مختلف التشريعات

---

[1] د/ محمود نجيب حسني، المرجع السابق، ص 774.

المقارنة، ثمّ نحدّد نطاق تطبيقه، وما إذا كان يقتصر على مرحلة المحاكمة ــ باعتبارها المرحلة المقرّرة للفصل في الدعوى ــ أم أنه يمتدّ ليشمل المرحلة السابقة عليها كذلك، أيْ مرحلة التحقيق الابتدائي، استنادا إلى أنّ كل مرحلة إنما تفترض تقديرا معيّنا لعناصر الإثبات.

أـ تعريف مبدأ الاقتناع القضائي: تعدّدت الآراء فيما يتعلّق بيان مدلول الاقتناع القضائي[1][2]، إلاّ أنّها في النهاية تصبو إلى معنى واحد وهي: أنّ للقاضي أن يستمدّ عقيدته من أيّ دليل يطمئن إليه، سواء من تلك الأدلة التي طرحت عليه من قبل النيابة العامة أو الخصوم، أو التي يرى بنفسه تقديمها، ليكوّن منها قناعته في الحكم، وهذه الحريّة التي يتمتّع بها القاضي الجنائي غير مقرّرة بهدف توسيع سلطته من حيث الإدانة أو البراءة، وإنّما هي مقرّرة له بالنظر إلى صعوبة الحصول على الدليل في المواد الجنائيّة.

وقد أقرت معظم التشريعات الحديثة[3] هذا المبدأ، حيث نصّ عليه المشرّع الفرنسي لأوّل مرّة في المادة (342) من قانون التحقيقات الجنائيّة، وذلك من خلال التعليمات التي تلقى على المحلّفين قبل خلوهم للمداولة، وإذا كان هذا النصّ قد أُلغيَ بمقتضى قانون 25 نوفمبر 1941،إلاّ أنّ تطبيقه لم يختلف، لأنّ هذه المادة نقلت حرفيّا في المادة (353) من قانون

---

[1] يعرّف الاقتناع لغة على أنّه: الاطمئنان إلى فكرة ما، أي قبولها. فقد جاء في لسان العرب تحت مادة "قنع": قنع بنفسه قنعا وقناعة بمعنى رضي. وفي القاموس المحيط: والقناعة: الرضي. وفي مختار الصحاح: "والقناعة الرضا بالقسم"، وبابه سلم، فهو قنعٌ وقنوع وأقنعه الشيء، أي أرضاه. وورد في المعجم الوجيز: يقال اقتنع، قنع، واقتنع بالفكرة أو الرأي أي قبله واطمئنّ إليه. انظر على الترتيب: ابن منظور، لسان العرب، الجزء الثامن، دار صادر، بيروت، ص 297. القاموس المحيط، الجزء الأول ، الطبعة الأولى، المكتبة العلميّة، بيروت، 1981، ص 135. مختار الصحاح، مكتبة لبنان ناشرون، بيروت، 1995، ص 231. المعجم الوجيز، مجمع اللغة العربيّة، طبعة خاصة بوزارة التربية والتعليم، 1990، ص 518.

[2] حيث عرّفه الدكتور محمود مصطفى بأنّه "التقدير الحر المسبب لعناصر الإثبات في الدعوى وهو البديل عن نظام الأدلة القانونيّة"، وفي رأي ليوني جيوفاني "أنّ الاقتناع الحر للقاضي لا معنى له أكثر من أنّه سلطة القاضي وواجبه في أن يستمدّ من أيّ مصدر وسيلة إثبات الوقائع، وأن يقدّرها دون أن يقيّده في ذلك حدّا أو قيدا ما"، ويرى آخرون أنّه عبارة عن حالة ذهنيّة ذاتيّة تستنتج من الوقائع المعروضة على بساط البحث عن احتمالات ذات درجة عالية من التأكد الذي تصل إليه نتيجة استبعاد الشك بطريقة قاطعة". انظر على الترتيب: د/ محمود محمود مصطفى، المرجع السابق، ص 95. ليوني جيوفاني، مبدأ الاقتناع والمشاكل المرتبطة به، المرجع السابق، ص 923. د/ إبراهيم الغماز، المرجع السابق، ص 627.

[3] لم يقتصر تطبيق مبدأ الاقتناع القضائي على التشريعات اللاتينية فحسب، بل يمتدّ حتى بالنسبة للتشريعات الانجلوأمريكيّة مع اختلاف طفيف في الصياغة، فهي لا تعرف تعبير الاقتناع القضائي، وإنّما تستخدم بدلا منه **تعبير ثبوت الإدانة بعيدا عن أيّ شك معقول (Proof beyond a reasonable doubt)** . انظر:
Spencer(John), la preuve en procédure pénale, droit englais, R.I. D. P, 1992, p. 101.

الإجراءات الحالي الصادر في 1958[1]، التي تنص على ما يلي: " لا يطلب القانون من القضاة حسابا بالأدلة التي اقتنعوا بها، ولا يفرض قاعدة خاصّة تتعلّق بتمام وكفاية دليل ما، وإنّما يفرض عليهم أن يتساءلوا في صمت وتدبّر، وأن يبحثوا في صدق ضمائرهم أي تأثير قد أحدثته الأدلة الراجحة ضد المتّهم ووسائل دفاعه..."[2].

وتنطبق هذه القاعدة أمام كل الجهات القضائيّة الجنائيّة، حيث كرّست بالمادتين (427 و536) من قانون الإجراءات الجنائيّة الفرنسي، فالمادة (427) هذه تطبّق أمام محكمة الجنح، أما المادة (536) تنطبق أمام محكمة المخالفات، حيث تحيل إلى تطبيق المادة(427) .

أمّا المشرع الجزائري فإنّه كرّس مبدأ الاقتناع القضائي بموجب المادة (307) من قانون الإجراءات، وهي مستوحاة من المادة(353)من القانون الفرنسي حيث تنص على:" يتلوا الرئيس قبل مغادرة المحكمة قاعة الجلسة التعليمات الآتية التي تعلّق فضلا عن ذلك بحروف كبيرة في أظهر مكان غرفة المداولة:(إنّ القانون لا يطلب من القضاة أن يقدموا حسابا على الوسائل التي بها قد وصلوا إلى تكوين اقتناعهم، ولا يرسم لهم قواعد بها يتعيّن عليهم أن يخضعوا لها على الأخص تقدير تمام أو كفاية دليل ما، ولكنه يأمرهم أن يسألوا أنفسهم في صمت أن يبحثوا بإخلاص ضمائرهم في أي تأثير قد أحدثته في إدراكهم الأدلة المسندة إلى المتّهم وأوجه الدفاع عنها ولم يضع لهم القانون سوى هذا السؤال الذي يتضمّن كل مطاق واجباتهم: هل لديكم اقتناع شخصي؟).

كما أنّ الاقتناع القضائي كرسته أيضا صراحة المادة (212) من قانون الإجراءات الجزائيّة الجزائري حيث تنص :" يجوز إثبات الجرائم بأي طريقة من طرق الإثبات ما عدا الأحوال التي ينص فيها القانون على غير ذلك، وللقاضي أن يصدر حكمه تبعا لاقتناعه الخاص..".

---

[1] Stefani(Gaston)، preuve، in Dalloz répertoire de droit pénal، et de procédure pénal، tome v، 1969، p. 5.

[2] Article 535 du (C.P.P) ، dispose que :" La loi ne demande pas compte aux juges des moyens par lesquels ils se sont convaincus، elle ne leur prescrit pas de règles desquelles ils doivent faire particulièrement dépendre la plénitude et la suffisance d'une preuve ; elle leur prescrit de s'interroger eux-mêmes dans le silence et le recueillement et de chercher، dans la sincérité de leur conscience، quelle impression ont faite، sur leur raison، les preuves rapportées contre l'accusé، et les moyens de sa défense. La loi ne leur fait que cette seule question، qui renferme toute la mesure de leurs devoirs: "Avez-vous une intime conviction ?".

وفي نفس السياق تحرص المحكمة العليا على ضرورة مراعاة مبدأ اقتناع القضائي وتوصي بإعماله أمام المحاكم الجنائية [1].

وقد ورد المبدأ ذاته في المادة (1/302) من قانون الإجراءات الجنائيّة المصري حيث نصّت على أنّه: "يحكم القاضي في الدعوى حسب العقيدة التي تكوّنت لديه بكامل حريّته ". وتؤكد هذا المبدأ أيضا المادتين (1/291و300) من هذا القانون، وهما يشيران بجلاء إلى الدور الايجابي للقاضي الجنائي وعدم اقتصاره على ما يقدمه له الخصوم، وذلك من أجل وصوله إلى الحقيقة الفعليّة في الدعوى.

وفي ذلك تقول محكمة النقض المصريّة في قضاء مستقر أنّ "العبرة في المحاكمات الجنائيّة هي باقتناع القاضي بناء على الأدلّة المطروحة عليه بإدانة المتهم أو ببراءته ولا يصح مطالبته بالأخذ بدليل دون دليل، كما أنّه من المقرّر أنّ لمحكمة الموضوع كامل الحريّة في أن تستمدّ اقتناعها من أيّ دليل تطمئن إليه طالما أنّ له مأخذا صحيحا من أوراق الدعوى... "[2].

ب ـ نطاق تطبيق مبدأ الاقتناع القضائي: لقد ثار خلاف حول المجال الحقيقي لتطبيق مبدأ الاقتناع القضائي، سواء من حيث طبيعة القضاء، أو من حيث مراحل الدعوى الجنائيّة.

فبالنسبة للأولى: يمتدّ تطبيق مبدأ الاقتناع القضائي إلى كافة أنواع المحاكم الجنائيّة، سواء كانت محاكم الجنايات أم الجنح أم المخالفات، وإن كان المشرّعان الجزائري والمصري لم يحدّدا ذلك صراحة في المواد المقرّرة لهذا المبدأ[3]، بخلاف المشرّع الفرنسي، فقد صرّح ذلك صراحة، حيث خصّص المادة(1/353) من قانون الإجراءات لتطبيق المبدأ أمام محكمة الجنايات، كما نصّت المادة (427) من ذات القانون على تطيق هذا المبدأ بالنسبة لمحاكم الجنح، أما المادة (536) من نفس القانون فهي مخصّصة بالنسبة لمحاكم المخالفات. وهو ما لم يقم به المشرع البلجيكي مثلا[4].

---

[1] المحكمة العليا الجزائريّة، الغرفة الجنائيّة، بتاريخ 28 فبراير 1968، المجلة الجزائريّة للعلوم القانونية ، 1968، ص 554. 9 جويلية 1981، مجموعة قرارات الغرفة الجنائيّة، ص 56. 13 ماي 1986، رقم 304، غير منشور ، اطلع عليه في تقنين الإجراءات ، تحت إشراف نواصر العايش، ص 90.

[2] نقض 2 أبريل 1973، مجموعة أحكام النقض، س 24، رقم 97، ص 471. نقض 8/ 2/ 1998، مجموعة أحكام النقض س 49 رقم 28، ص 188. نقض 25/ 3/ 1998، رقم 62 ص 479. نقض 23/ 3/ 2000 الطعن رقم 21505 لسنة 61، ق. نقض 10/ 5/ 2004 الطعن رقم 12583 لسنة 62 ق.

[3] راجع المواد (307 و212) من قانون الإجراءات الجزائيّة الجزائري، أيضا (1/302 و291) من قانون الإجراءات الجنائيّة المصري.

[4] حيث نصّ على هذا المبدأ ضمن الأحكام الواردة في الباب المتعلّق بمحكمة الجنايات، وهو ما دفع بعض الفقهاء البلجيكيين إلى القول بأنّ مبدأ الاقتناع القضائي لا ينطبق إلاّ أمام محكمة الجنايات ويرفضون تطبيقه أما قضاء التحقيق وكذا محكمة الجنح والمخالفات. انظر: ==

أمّا بالنسبة للثانية: فإذا كان مبدأ الاقتناع القضائي شُرع أصلا لكي يطبّق أمام قضاء الحكم، إلاّ ذلك لا يعني أبدا أنّ نطاق تطبيقه مقصور على هذه المرحلة، بل هو يمتد كذلك ليشمل مرحلة التحقيق الابتدائي[1]، حيث أنّ هذا المبدأ يطبّق أيضا أمام قضاة التحقيق والإحالة، فهم يقدّرون مدى كفاية الأدلة أو عدم كفايتها للاتهام، دون الخضوع لقواعد معيّنة ولا لرقابة محكمة النقض ولكنّهم يخضعون في ذلك لضمائرهم واقتناعهم الذاتي فحسب. أمّا قضاة الحكم فهم يقدّرون الأدلة من حيث كفايتها أو عدم كفايتها للحكم بالإدانة، وبذلك يمكن القول بأنّ الأولى تسعى إلى ترجيح الظن أمّا الثانية تسعى إلى توكيد اليقين. ويترتّب على ذلك نتيجة هامة، وهي أنّ الشك في مرحة الاتهام يفسّر ضدّ مصلحة المتّهم، بينما يكون في صالحه في مرحلة الحكم[2].

وقد قضت محكمة النقض المصريّة بأنّ المقصود من كفاية الأدلة في قضاء الإحالة أنّها تسمح بتقديم المتّهم للمحاكمة مع رجحان الحكم بإدانته وهو المعنى الذي يتّفق ووظيفة ذلك القضاء كمرحلة من مراحل الدعوى الجنائيّة[3].

ثانيا- قيمة الدليل الالكتروني كدليل علمي:

في البداية ينبغي علينا الإشارة إلى الدليل الالكتروني لا يحظ أمام القاضي الجنائي بقوّة حاسمة في الإثبات، وإنّما هو مجرد دليل لا تختلف قيمته ولا تزيد حجّته عن سواه، وهذا أثر من آثار حريّة القاضي الجنائي في الاقتناع، وعلى هذا الأساس يصح للقاضي أن يؤسس اقتناعه على الدليل الالكتروني كما يصح أن يهدره تبعا لاطمئنانه، ولا يجوز مطالبة القاضي أو إلزامه بالاقتناع بالدليل الالكتروني ولو لم تكن في الدعوى أدلة سواه.

وتجدر الإشارة إلى أنّ الفقه الفرنسي يتناول حجية مخرجات الكمبيوتر في المواد الجنائية ضمن مسألة قبول الأدلة المتحصلة عن الآلة أو ما يسمى بالأدلة العلمية، سواء كانت بيانات

== - R .Legros، la preuve légale en droit pénale، in la preuve en droit Bruxelles،1981، p. 149 à 175.

مشار إليه عند: د/ محمد مروان، المرجع السابق، ص 467.

[1] ويستخلص ذلك ضمنا من أحكام المادة (2/162) من قانون الإجراءات الجزائيّة الجزائري، إذ تنص "...يمحّص قاضي التحقيق الأدلة وما كان يوجد ضد المتّهم دلائل مكوّنة لجريمة من جرائم العقوبات". وكذلك من أحكام المادة (1/163) حيث تنص على أنّه: " إذا رأى قاضي التحقيق أنّ الوقائع لا تكون جناية أو جنحة أو مخالفة أو أنّه لا توجد دلائل كافية ضد المتّهم أو كان مقترف الجريمة ما يزال مجهولا أصدر أمر بأن لا وجه لمتابعة المتّهم ...".

[2] د/ إبراهيم الغماز، المرجع السابق، ص 644.

[3] نقض 25 أبريل سنة 1967، مجموعة أحكام النقض، س 18، رقم 13، ص 569.

مكتوبة أو صورا. وتطبيقا لذلك قضي في فرنسا بخصوص قوّة المحرّرات الصادرة عن الآلات الحديثة في الإثبات بأنّه إذا كانت التسجيلات الممغنطة لها قيمة الدلائل يمكن الاطمئنان إليها، ويمكن أن تكون صالحة في الإثبات أمام القضاء الجنائي[1]. وفي حكم أخر قرّرت محكمة النقض الفرنسيّة بأنه إذا اطمأنت محكمة الموضوع وفقا لاقتناعها الذاتي والقواعد العامة إلى ما استندت إليه النيابة من قرائن بشأن خطأ سائق سيارة منسوب إليه تجاوز السرعة، وقد ثبت ذلك من خلال جهاز آلي التقط صورة السيارة المتجاوزة للسرعة، ودون أن يكون السائق قد سئل، فإنّها لا تكون ملزمة بتحديد من استندت إليه من عناصر الواقعة في تبرير اقتناعها[2].

ومن الجدير بالذكر أنّ أغلب التشريعات ذات الأصل اللاتيني وان كانت تتفق حول قبول الدليل الالكتروني استنادا إلى قاعدة الاقتناع الحر للقاضي الجنائي، إلاّ أنّها تختلف في طريقة تقديم هذا الدليل أمام المحكمة، حيث تشترط بعض التشريعات كالقانون اليوناني (المادة 324 من التقنين الإجرائي)[3] والياباني[4]، سويسري والنمساوي، قواعد معيّنة في هذا الخصوص، كأن يكون الدليل الالكتروني مقروءا سواء أكان مطبوعا على ورق بعد خروجه من الجهاز، أم كان مقروءا على شاشة جهاز الكمبيوتر ذاته.

وبما أنّ الدليل الالكتروني تطبيق من تطبيقات الدليل العلمي، وذلك بما يتميّز به من موضوعيّة وحياد وكفاءة، ممّا يجعل اقتناع القاضي الجنائي أكثر جزما ويقينا، حيث يساعده على التقليل من الأخطاء القضائيّة، والاقتراب إلى العدالة بخطوات أوسع، والتوصل إلى درجة أكبر نحو الحقيقة. تلك السمات التي ربما تدفع البعض إلى الاعتقاد بأنّه بمقدار اتساع مساحة الأدلة العلميّة ومن بينها الدليل الالكتروني بمقدار ما يكون انكماش وتضاؤل دور القاضي

---

(1) Crim 24avril 1987، Bull، n° 173.cité par Francillon(Jacques)، les crimes informatiques et d'autre crime dans le domaine de la technologie informatique en France، revue internationale du droit pénale، 1993، p. 308 et s.

(2)Crim 3 janvier 1978، Bul، n°1 ،Dalloz ، code de procédure pénale، 1991- 1992، p. 413. Crim، 20 janvier 1977، J.C. P. 1977، n° 11.

مشار إليه عند: د/ هشام محمد فريد رستم، الجوانب الإجرائيّة للجرائم المعلوماتية، دراسة مقارنة، المرجع السابق، ص 156.

(3) حيث تشترط المادة (364) من التقنين الإجرائي اليوناني قراءة المستندات والوثائق التي استخدمت كأدلة أثناء التحقيقات، مع العلم أنّه يسود مبدأ حريّة قبول الأدلة وحريّة تقييمها من طرف القاضي الجنائي (المادة 177– 179 إجراءات يوناني)

(4) ويجب التنويه بأنّ التسجيل الالكترومغناطيسي (Électro- magnétique) لا يصلح كدليل يستند منه القاضي اقتناعه بسبب أنه غير مرئي في حد ذاته، لدى يتم تحويلها إلى شكل مرئي مقروء عن طريق طباعتها، ومن تمّ قابليتها للتقدير. انظر: د/ هشام محمد فريد رستم، المرجع السابق، ص 159.

الجنائي في التقدير، خاصّة أمام نقص الثقافة الفنيّة للقاضي وبالتالي فإنّ مهمّته تصبح شبه آلية، حيث يكون الدور الأكبر للخبير الذي يسيطر على العمليّة الإثباتيّة، ولم يبق أمام القاضي سوى الإذعان لرأي الخبير، دون أيّ تقدير من جانبه.

وحقيقة إنّ المشكلة التّي تثار هنا ليست على درجة كبيرة من الأهميّة، خاصّة إذا قلنا بأنّ نظام الإثبات السائد يقوم على التوازن بين الإثبات العلمي والاقتناع القضائي، بحيث يُعمل بالإثبات العلمي في إطار مبدأ الاقتناع القضائي، ويمكن النظر إلى هذه المشكلة وتحليلها على ضوء بيان دور الخبير في الدعوى الجنائيّة من جهة، ثمّ تقدير القاضي للدليل العلمي من جهة أخرى.

1ـ دور الخبير في الدعوى الجنائيّة:

سبق الحديث عن الخبرة وبيان الدور البارز لها في عمليّة الإثبات القضائي نظرا لما شهده هذا العصر من تطور علمي وتكنولوجي[1]، لحد وصفه بعصر المعلومات. فالخبرة وسيلة إثبات تهدف إلى كشف بعض الدلائل والأدلة، أو تحديد مدلولها بالاستعانة بالمعلومات العلميّة[2]، التي لا تتوافر لدى القاضي، حيث تتطلب بعض الحالات معرفة خاصّة لا يملك القاضي الأهلية اللازمة لها، ممّا استلزم أن يكون للخبير دور في الدعوى الجنائيّة.

والدليل العلمي شأنه شأن باقي أدلة الإثبات يخضع لتقدير القاضي ومدى تأثيره في الاقتناع الذاتي للقاضي الجنائي، وأنّه لا يمكن للخبير مهما كانت دقّة نتائجه وموضوعيتها أن يحتل مكانة القاضي في إيجاد العدالة، والتي يستلزم إيجادها حسا مختصا لا يدركه غيره، ويتمّ هذا الحس من خلال التكوين العلمي والقضائي الرفيع، والذي تنهض به المؤسسات العلميّة القانونيّة بوجه عام والقضائيّة بوجه خاص، ليشكل أساسا رصينا في التقدير السليم للأدلة والذي من خلاله يصل إلى قراره العادل الذي يكون عنوانا للحقيقة.

2ـ تقدير القضاء للدليل العلمي:

يخضع الدليل العلمي ــ كما سبق ــ إلى تقدير القاضي الجنائي وبالتالي اقتناعه، وفي هذا الخصوص ينبغي أن نميّز بين أمرين:

ــ أوّلا: القيمة العلميّة القاطعة للدليل[3]:

---

(1) انظر فيما سبق، ص86 وما بعدها.

(2) د/ أحمد فتحي سرور، الوسيط في الإجراءات الجنائيّة، المرجع السابق، 494.

(3) د/ أبو القاسم، الدليل المادي، المرجع السابق، ص 307. د/ جميل عبد الباقي الصغير، المرجع السابق، ص 22 . وانظر أيضا: د/ هلالي عبد الله، حجيّة المخرجات الكمبيوترية في المواد الجنائيّة، دراسة مقارنة، الطبعة الأولى، دار النهضة العربيّة، 1997، ص 46.

ـ ثانيا: الظروف والملابسات التي وجد فيها الدليل: فتقدير القاضي لا يتناول الأمر الأوّل، وذلك لأنّ قيمة الدليل تقوم على أسس علميّة دقيقة، وبالتالي لا حريّة للقاضي في مناقشة الحقائق العلميّة الثابتة [1]. أمّا الظروف والملابسات التي وجد فيها الدليل، فإنّها تدخل في نطاق تقديره الذاتي، فهي من صميم وظيفته القضائيّة، بحيث يكون في مقدوره أن يطرح مثل هذا الدليل – رغم قطعيّته – إذا تبيّن بأنّه لا يتفق مع ظروف الواقعة وملابساتها، حيث تولد الشبهة لدى القاضي، ومن ثمّ يقضي في إطار تفسير الشك لصالح المتّهم.

ذلك أن مجرد توافر الدليل العلمي لا يعني أنّ القاضي ملزم بالحكم بموجبه مباشرة سواء بالإدانة أم بالبراءة، دون بحث الظروف والملابسات، فالدليل العلمي ليس آلية معدّة لتقرير اقتناع القاضي بخصوص مسألة غير مؤكدة[2]، بل هو دليل إثبات قائم على أساس من العلم والمعرفة، وللقاضي النظر إليه على ضوء الظروف والملابسات المحيطة.

وعلى ذلك، فإنّنا لا نذهب مع الاتجاهات الفقهيّة القائلة بأنّ نظام الأدلة العلميّة سيكون نظام المستقبل وسيحل الخبير في القضاء، فيكون الدور له وليس للقاضي، فيجعل رأي الخبير هو الحاسم لاقتناع القاضي. لكنّنا نقول أنّ التطور العلمي في مجال الأدلة لا يتعارض مع سلطة القاضي الجنائي في تقديرها، بل إنّ هذه الأدلة ستكفل للقاضي وسائل فعالة في كشف الحقيقة[3].

---

(1) أصبح للبصمة الوراثية (D.N.A) نتائج قاطعة في تحديد الهويّة، فعلى سبيل المثال، إذا أثبت فحص الحمض النووي استحالة أن يكون الطفل (س) ابنا للأب (أ) التي تدعي الأم (ب) نسبته إليه، فما على القاضي سوى التسليم لهذه النتيجة دون مناقشة كيف تمّ التوصل إلى هذه النتيجة من الناحيّة العلميّة، ونتيجة لذلك أصبحت بعض التشريعات مثل القانون الفرنسي، القانون الألماني، والقانون الايرلندي تستخدم البصمة الوراثية في التعرف على شخصيّة الجناة، وذلك بضمانات تحمي السلامة الجسديّة وحرمة الحياة الخاصة للمتّهم. لمزيد من التفصيل حول هذا الموضوع انظر: د/ جميل عبد الباقي الصغير، المرجع السابق، ص 59. وانظر أيضا: محمد أحمد غانم، الجوانب القانونيّة والشرعيّة للإثبات الجنائي بالشفرة الوراثيّة، دار الجامعة الجديدة، 2008، ص 207. وانظر أيضا: خالد محمد الحمادي، المرجع السابق، ص 29 وما بعدها .

(2) د/ جميل عبد الباقي الصغير، المرجع السابق، ص 23. د/ هلالي عبد الله، المرجع السابق، ص 47.

(3) د/ فاضل زيدان، المرجع السابق، ص 155.

الفرع الثاني

مدى تأثير مشكلات الدليل الالكتروني على اقتناع القاضي

يثير الدليل الالكتروني العديد من المشكلات، وهي في الحقيقة تتعلق بطبيعته التكوينية من جهة وبإجراءات الحصول عليه من جهة أخرى، وهذه المشكلات تعود عليه بالسلب حيث تضعف من قيمته في مجال الإثبات الجنائي إن لم يتّم إيجاد حلول بشأنها. وسيكون تناولنا لهذه المشكلات من خلال نوعين من المشاكل أولها موضوعيّة وثانيها مشكلات إجرائيّة.

أوّلا- المشكلات الموضوعيّة للدليل الالكتروني:

وهي غالبا ما تتعلّق بطبيعة الدليل ذاته، وذلك بسبب الخصائص الفيزيائية التي يتكوّن منها هذا الدليل، سواء بسبب الطبيعة غير المرئية له، أو بسبب مشكلة الأصالة، أو بسبب ديناميكيّته.

1- **الدليل الالكتروني دليل غير مرئي:** فهو عبارة عن سجل كهرومغناطيسي مخزن في نظام حاسوبي في شكل ثنائي[1]، وبطريقة غير منظمة، فعلى سبيل المثال تتضمن الأقراص الصلبة مزيجا من بيانات مختلطة فيما بينها والتي لن تكون كلها ذات صلة بالمسألة المطروحة [2]، بمعنى أنّ هناك اختلاطا بين الملفات البريئة مع تلك المجرمة التي تعدّ موضوعا للدليل الجنائي الرقمي ممّا تؤدي إلى خلق مشكلة التعدي على الخصوصية. وبالتالي يختلف الدليل الرقمي عن الآثار المادية الناتجة عن الجرائم التقليدية كالأعيرة والأسلحة النارية أو المحرر ذاته الذي تمّ تزويره، ممّا يسهل على رجال العدالة إثباتها، بعكس الجرائم الالكترونية حيث يكون ذلك في منتهى الصعوبة، بل الدليل فيها – الدليل الرقمي – عبارة عن نبضات الكترونية مكوّنة من سلسلة طويلة من الأصفار، لا تفصح عن شخصية معينة، وهذه المشكلة تظهر بصفة جلية مع شبكه الانترنت حيث تسمح لمستخدميها الاتصال بدون الكشف عن أسماءهم الحقيقية كإرسال رسائل البريد الالكتروني مجهولة المصدر، فضلا عن ذلك غالبا ما يكون الدليل الرقمي مرمّزا أو مشفرا، كما يمكن تعديله والتلاعب فيه، مما يقطع الصلة بين

---

(1) Computer Forensics Procedures، Tools, and Digital Evidence Bags Brett Pladna, What They Are and Who Should Use Them. available at:
http://www.infosecwriters.com/text_resources/pdf/BPladna_Computer_Forensic_Procedures.pdf.

(2) Johann Hershensohn، I.T. FORENSICS: THE COLLECTION AND PRESENTATION OF DIGITAL EVIDENCE، available at :
http://icsa.cs.up.ac.za/issa/2005/Proceedings/Full/076_Article.pdf

المجرم وجريمته، ويحول دون كشف شخصيته، وبذلك يشكل هذا الدليل عائقا امام رجال التحرّي والتحقيق خاصة أنهم اعتادوا على الإثبات المادي للجرائم.

2ـ **مشكلة الأصالة في الدليل الالكتروني:** إنّ الأصالة في الدليل الالكتروني لها طابع افتراضي لا يرتقي إلى مستوى الأصالة في الدليل المادي، فهذه الأخيرة تعبير عن وضعية ماديّة ملموسة، كما هو الشأن في الورق المكتوب أو بصمة الأصبع، في حين أن الدليل الرقمي عبارة عن تعداد غير محدود لأرقام ثنائية (Binary Digits) موحدة في الصفر والواحد (0 - 1) فالصورة (Image) مثلا في العالم الرقمي ليس لها ذلك الوجود المادي الذي نعرفه في شكل ورقي، وإنما هي مجموعة من الأرقام التي ترجع إلى أصل واحد هو الرقم الثنائي المشار إليه، فكل شيء في العالم الرقمي يتكوّن من الصفر والواحد وهما في تكوينهما الحقيقي عبارة عن نبضات متواصلة الإيقاع تستمد حيويتها و تفاعلها من الطاقة. ولقد أثارت مسألة الأصالة العديد من المشكلات من حيث مدى الاعتداد بالنسخة التي تشكل دليلا كاملا هنا.

والواقع من الأمر أنّ بحث موضوع الأصالة على المستوى القانوني جعل المشرع المقارن يعتمد منطق **افتراض أصالة الدليل الالكتروني**، وقد تضمن قانون الإجراءات الجنائية الفدرالي في الولايات المتحدة الأمريكية نصا صريحا (القاعدة 1001بند (3) حيث يسمح استثناء بقبول الدليل الالكتروني باعتباره مستندا أصليا مادام أن البيانات صادرة من كمبيوتر أو جهاز مماثل وسواء أكانت هذه البيانات مطبوعة أم مسجلة على دعامات أخرى ومقروءة للعين المجردة وتعبّر عن البيانات الأصلية بشكل دقيق[1]. ومنه تتساوى الكتابة الماديّة من حيث الأصالة مع مخرجات الحاسوب على الرغم من أنّ طبيعة الكتابة عبر الحاسوب تجعل من المخرجات مجرد نسخ للأصل الموجود رقميا في الحاسوب أو عبر الانترنت .

3ـ **الدليل الالكتروني ذو طبيعة ديناميكية** : فهو ينتقل عبر شبكات الاتصال بسرعة فائقة، بمعنى إمكانية تخزين المعلومات أو البيانات في الخارج بواسطة شبكة الاتصال عن بعد، ويترتب على ذلك صعوبة تعقّب الأدلة الرقمية وضبطها، لأنّه يستلزم القيام بأعمال إجرائية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها[2]، مثل معاينة مواقع الانترنت المخالفة، تفتيش نظم الحاسب الآلي، أو ضبط الأقراص الصلبة التي تحتوي على مواد غير مشروعة كالصور الإباحية مثلا، وهذا كله يصطدم بمشاكل الحدود والولايات القضائية، ويرجع السبب في ذلك إلى أنّ هذه الإجراءات تمثل مساسا بسيادة الدولة التي عبر من خلالها

---

(1) Pascal Vergucht ، op. cit، p. 120.

(2) Marthew. R . Zakaras، International Computer Crime, revue international de droit pénal, 3 eme et 4eme trimestres 2001 ، p 828 .

نشاط المجرم وهو في طريقه للهدف، أو حيث قد توجد أدلة الجريمة، وهو ما ترفضه الغالبية العظمى من الدول، لذلك أبرمت العديد من الاتفاقيات والمعاهدات الدولية في مجال التعاون الدولي[1] التي تستهدف من وراء ذلك التقريب بين القوانين الجنائية الوطنية من اجل جمع هذا النوع من الأدلة العابرة للحدود خاصة في إطار مكافحة الجرائم العالمية ومنها الجرائم الالكترونية .

ثانيا- المشكلات الإجرائيّة للدليل الالكتروني:

لا تقف مشكلة الدليل الالكتروني عند طبيعته التكوينية، بل تمتد لتشمل إجراءات الحصول عليه، وتتمثل هذه الأخيرة في حالتين هما: ارتفاع تكاليف الحصول عليه، ممّا أدى إلى القول بأنّ الدولة، على الرغم من أنّ مسعاها الحقيقي هو تحقيق العدالة، لن تلجأ إلى أسلوب الإنفاق في هذا الإطار[2]. أمّا المشكلة الثانية تتعلق بنقص الخبرة الفنية و التقنية لدى سلطات الاستدلال والتحقيق والقضاء بمجال تقنية المعلومات. كل ذلك سنتعرض له من خلال النقاط التالية:

1 **- ارتفاع تكاليف الحصول على الدليل الالكتروني:** غالبا ما يتمّ اللجوء إلى الخبرة في مجال التعامل مع أيّ ظاهرة فنية، لاسيما في مجال تكنولوجيا المعلومات والانترنت، فهي تؤدي دور لا يستهان به إزاء نقص معرفة رجال إنفاذ القانون للجوانب التقنية في الجرائم الالكترونية، إلاّ أنّ هذه الخبرة تشكل عبئا ثقيلا على العدالة الجنائية بالنظر إلى حجم وضخامة المصاريف

---

[1] مثل الاتفاقية الأوربية للإجرام المعلوماتي (اتفاقية بودابست) الموقعة في 2001/11/23 ، حيث تمّ تخصيص الباب الثالث لدراسة التعاون الدولي Coopération International ، ومن خلاله نصت **المادة 23** "على ضرورة تعاون الأطراف فيما بينها وفقا لأحكام هذا الفصل، ومن خلال تطبيق الوسائل الدولية الملائمة بالنسبة للتعاون الدولي في المسائل الجنائية و الترتيبات التي تستند إلى تشريعات موحدة ومتبادلة، وكذلك بالنسبة للقوانين المحلية، إلى أقصى مدى ممكن، بغرض التحقيقات و الإجراءات الجنائية المتعلقة بالجرائم ذات الصلة بالنظم الحاسوبية و البيانات المعلوماتية، أو لجمع الأدلة ذات الشكل الالكتروني لمثل هذه الجرائم " .

Article 23 . General principles relating to international co-operation

"The Parties shall co-operate with each other، in accordance with the provisions of this chapter، and through the application of relevant international instruments on international co-operation in criminal matters، arrangements agreed on the basis of uniform or reciprocal legislation، and domestic laws، to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data، or for the collection of evidence in electronic form of a criminal offence".

[2] د / عمر محمد ابوبكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، المرجع السابق ، ص 984 .

التي يتمّ إنفاقها في سبيل الحصول على الدليل الرقمي، وان كان الإنفاق يتفاوت حسب ما إذا كانت الدولة تأخذ بالنظام الاتهامي أو بنظام التنقيب والتحري[1]، غير أن الإشكال الأساسي لا يتعلق بطبيعة النظام الإجرائي المتّبع في كل دولة، و إنّما ينحصر في طبيعة الدليل الرقمي وما يتطلب إثباته من تكاليف باهظة، خاصة أمام غياب منظمات متخصصة كالجامعات والمعاهد لاسيما في الدول العربية حيث يتطلب الأمر اللجوء إلى شركات أو منظمات أجنبية في الخارج، ممّا يجعل التكاليف تخضع للسعر العالمي المقرر في اللوائح المالية لتلك المنظمات .

لذلك نقترح إنشاء مخابر معتمدة تابعة للأجهزة العدالة الجنائية، تكون مجهزة بأحدث وسائل التقنية، مع ضرورة تبادل المعلومات مع المراكز والمؤسسات الأجنبية حكومية كانت أم خاصة حتى تستفيد من خبراتها في المجال التقني لاسيما تجربة الولايات المتحدة الأمريكية باعتبارها من الدول السباقة في هذا المجال، وذلك عن طريق الندوات والمؤتمرات، فضلا عن دورات تدريبية وذلك في إطار التعاون الدولي الذي يستهدف تقريب وجهات النظر وتوحيد المفاهيم بين الدول المختلفة، والتعرف على أحدث التطورات من خلال تبادل الخبرات لاسيما أمام **الفجوة الرقمية** [2] التي يعيشها سكان العالم خاصّة بين الدول المتقدمة والدول النامية، في إطار استخدام نظم تكنولوجيا المعلومات ومدى إمكانية استيعاب السرعة في التطوير سواء من حيث القطع الصلبة أو البرمجيات

2 ـ **نقص المعرفة التقنية لدى رجال إنفاذ القانون:** إنّ الطبيعة الخاصة بالدليل في مجال الجريمة الالكترونية انعكس على عمل الجهات المكلّفة بالتحقيق والمحاكمة حيث يتطلّب الكشف عن هذه الجرائم وإثباتها إتباع استراتجيات خاصة تتعلق باكتسابهم مهارات خاصة على نحو يساعدهم على مواجهة تقنيات الحاسب الآلي وشبكاته، بحيث تتعقد التقنيات المرتبطة بارتكاب تلك الجرائم لذا يجب استخدام تقنيات تحقيق جديدة لتحديد نوعية الجريمة المرتكبة وشخصية مرتكبيها و كيفية ارتكابها مع الاستعانة بوسائل جديدة أيضا لضبط الجاني والحصول على أدلة إدانته[3]. لذا من المتصور أن تجد الجهات المكلفة بالقبض والتحقيق نفسها غير قادرة على

---

(1) د / عمر محمد أبوبكر بن يونس، نفس المرجع، ص 987 .

(2) الفجوة الرقمية هي: درجة التفاوت في مستوى التقدم (سواء بالاستخدام أو الإنتاج) في مجال الاتصالات وتكنولوجيا المعلومات بين بلد وأخر أو تكتل وأخر أو مناطق البلد الواحد. انظر ورقة عمل حول مؤشرات الفجوة الرقمية الأمانة العامة - لجامعة الدول العربية إدارة الاتصالات وتكنولوجيا المعلومات ـــ ، مقدمة للاجتماع الرابع عشر للفريق العربي للتحضير للقمة العالمية حول مجتمع المعلومات 17، في 18-/1/ 2005 متاح على الموقع التالي :

www.aticm.org.eg/admin/Farek_kema/itind.doc

(3) YANN PADOVA ،op. cit. p ،772 .

التعامل بالوسائل الاستدلالية والإجراءات التقليدية مع هذه النوعية من الجرائم، فكثيرا ما تفشل جهات التحقيق في جمع الأدلة الالكترونية، بل أنّ المحقق نفسه قد يدمّر الدليل بخطأ منه أو بإهمال، كقيام رجال الشرطة بوضع حقيبة كاملة تحتوي على اسطوانات الكمبيوتر المصادرة وذلك في صندوق السيارة بالقرب من جهاز الإرسال والاستقبال اللاسلكي فكانت النتيجة أن الإشارات الكهربائية القوية تسببت في تدميرها جميعا [1]. لذا يجب أن تنشأ كل دولة إدارة متخصصة بهذا النوع من القضايا، وذلك لتلقي البلاغات وملاحقة المجرم الالكتروني والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة [2].

وهو ما حدث فعلا، حيث أنشأت شرطة متخصصة لمكافحة هذا النوع المستحدث من الإجرام سواء على المستوى المحلي لكل دولة أو على المستوى الدولي .

1ـ **على المستوى الدولي:** لمّا كانت الجرائم الالكترونية عابرة للحدود، ويمكن أن تتعدى آثارها عدة دول، ممّا يستحيل على الدولة القضاء عليها بمفردها، لذلك فانّ الحاجة تدعو إلى ضرورة التعاون فيما بينها باعتباره إحدى الضرورات اللازمة لمواجهة هذه الأنشطة الإجرامية المستحدثة. ويعدّ التعاون الشرطي الدولي (La Coopération Policière International) من أهم صور التعاون الدولي في مكافحة الإجرام بصفة عامة والإجرام العابر للحدود لاسيما الإجرام الالكتروني بصفة خاصة، ويتحقق هذا التعاون من خلال عدة أجهزة من أهمها : **المنظمة الدولية للشرطة الجنائية " الانتربول"** [3] وتهدف هذه المنظمة إلى تأكيد و تشجيع التعاون بين أجهزة الشرطة في الدول الأطراف على نحو فعال في مكافحة الجريمة، وذلك عن طريق تجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة في أقاليم الدول المنظمة إليها، و تبادل هذه البيانات فيما بينها .

هذا وقد أكد سكرتير الانتربول الدولي" Raymond Kendall " في مؤتمر جرائم الانترنت المنعقد في لندن في 10/9/ 2000على ضرورة تعاون الدول في مكافحة جرائم الانترنت باعتبار هذه الأخيرة تبرز كظاهرة دولية، وقد أكّد على أنه يجب على المجتمع الدولي عدم

---

[1] د / عبد الله حسين محمد، المرجع السابق، ص 355.

[2] مهندس / رأفت رضوان، شرطة الانترنت، بحث منشور بمجلة بحوث الشرطة، العدد 26، يوليو 2004، ص111.

[3] أنشئ هذا الجهاز سنة 1923تحت اسم اللجنة الدولية للبوليس الجنائي، ثم تغير اسمه عام 1956 إلى المنظمة الدولية للبوليس الجنائي وتضم هذه المنظمة 160 دولة أعضاء فيها من بينها الجزائر و مصر. وللمزيد عن التفاصيل حول هذا الموضوع راجع في ذلك : سراج الدين الروبي، الانتربول وملاحقة المجرمين ، دار المصرية اللبنانية، 1998 .

الانتظار إلى حين عقد معاهدات واتفاقيات في هذا الإطار بل يجب الشروع وبشكل فوري في مكافحة هذه الجرائم[1] ، ويقوم الانتربول بوضع إستراتيجية جديدة لمواجهة جرائم الانترنت بالتعاون مع الأمم المتحدة، ويمكن القول بوجود سابقة تاريخية في هذا الإطار، وهي السابقة التي تعقبت فيها المباحث الفدرالية الأمريكية FBI بالاشتراك مع الانتربول، والمتعلقة بملاحقة الشخص الذي قام بنشر دودة الحب (LOVE BUG) عبر الانترنت في الفلبين[2]. وكذلك ما حصل في الجمهورية اللبنانية عندما تم توقيف أحد الطلبة الجامعيين من قبل القضاء اللبناني بتهمة إرسال صور إباحية لقاصرة دون العشرة أعوام من موقعه على شبكة الانترنت، وذلك أثر تلقي النيابة اللبنانية برقية من الانتربول في ألمانيا بهذا الخصوص [3] .

وتجدر الإشارة إلى انه وجود منظمات أخرى لها دور لا يقل عن دور الانتربول في مواجهة هذا النوع المستحدث من الإجرام على المستوى الدولي، كمنظمة التعاون الاقتصادي و التنمية (OECD) ومجموعة الثمانية الاقتصادية (G -8) Group of Eight Economies حيث قامت بإعداد ملتقى دولي في نهاية نوفمبر 2000 في طوكيو لتكوين قوة دولية أطلق عليها " The Digital Opportunity Task Force " تتمثل مهامها في تحقيق امن تكنولوجيا المعلومات/ الانترنت [4].

وعلى غرار هذه المنظمة أنشأ المجلس الأوربي في لوكسمبورغ عام 1991 **شرطة أوربية " الاوربول"** والتي تتخذ من لاهاي – هولندا – مقرا لها، لتكون همزة وصل بين أجهزة الشرطة الوطنية في الدول المنظمة و لملاحقة الجناة في الجرائم العابرة للحدود ومنها بطبيعة الحال الجرائم الالكترونية [5]، و للاوربول دور فعال في مكافحة جرائم الانترنت، حيث نجده يقوم بتسهيل التحقيقات المرتبطة بوقائع بث أو امتلاك محتويات إباحية عبر الانترنت بين الدول الأوربية، وقد تم عقد اجتماعات لمكافحة هذا النوع من الإجرام في جوان2001 في لاهاي، بالإضافة إلى اجتماعات أخرى بمشاركة السلطات القمعية الألمانية حول موضوع الاستغلال الجنسي للأطفال[6].

---

[1] د / عمر محمد ابوبكر بن يونس ،الجرائم الناشئة عن استخدام الانترنت ، المرجع السابق ، ص 814 .

[2] د / عمر محمد ابوبكر بن يونس، نفس المرجع، نفس الموضع .

[3] حول هذه الواقعة انظر جريدة النهار اللبنانية في عددها الصادر بتاريخ 19 / 7 / 2001 .

[4] د / عمر محمد ابوبكر بن يونس ، المرجع السابق ، ص 814 .

[5] د/ جميل عبد الباقي الصغير، الجوانب الإجرائية للجرائم المتعلقة بالانترنت، المرجع السابق، ص 79 .

[6] انظر: نبيلة هبة مولاي علي هروال ، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات ، دراسة مقارنة ، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2005 – 2006، ص 54 .

في 2002 /2/28 تمّ إنشاء "**الاورجست**" من قبل مجلس الاتحاد الأوربي، كجهاز يساعد على التعاون القضائي والشرطي في مواجهة الجرائم الخطيرة [1]، حيث يعد دعامة في فعالية التحقيقات والمطاردات المتبعة من قبل السلطات القضائية الوطنية، وخصوصا فيما يتعلق بالأنشطة المرتبطة بجرائم الانترنت[2].

– والى جانب الانتربول والاورجست، تمّ إنشاء فضاء جماعي من غير حدود (Espace Communautaire sans frontière) سمي **بشنجن** (SCENGEN)، وذلك من خلال التوقيع على معاهدة (SCENGEN) في14/ 1985/6 وعلى اتفاقية تطبيق تلك المعاهدة في (6/19/ 1990). وقد استحدثت هذه الاتفاقية وسيلتين جديدتين لتعزيز التعاون الشرطي الأوربي لمواجهة التحديات الأمنية التي تفرضها الظروف الجديدة، منها جرائم الانترنت وتتمثل هاتان الوسيلتان في مراقبة المشتبه فيهم عبر الحدود و ملاحقة المجرمين [3].

فضلا عن ذلك قام مركز التدريب الوطني عن الجرائم التقنية(NSLEC) وهو أحد المؤسسات التابعة للاتحاد الأوربي بإعداد المشروعات والبرامج الّتي تهدف إلى مكافحة الجرائم عالية التقنية، ومن أهم هذه المشروعات مشروع فالكون 2001، وأيضا برنامج أجيس 2003/ 2004. اللذان يهدفان إلى التدريب على مكافحة الجريمة المعلوماتية [4] .

أمّا على المستوى العربي نجد أنّ مجلس وزراء الداخلية العرب أنشأ المكتب العربي للشرطة الجنائية[5]، بهدف تأمين وتنمية التعاون بين أجهزة الشرطة في الدول الأعضاء في

---

(1) Nadine L.C Thwaites : Eurojust ، autre brique dans l'édifice de l coopération judiciaire en matière pénale ou solide mortier ?، revue de science criminelle et de droit pénale comparé، n 1 ، janvier - mars 2003 ، p 45 .

(2) ويتمثل أهم نشاطات الاورجست في: تحسين التنسيق و التعاون بين السلطات القضائية المختصة للدول الأطراف، تبادل المعطيات بين دول أعضاء الاتحاد الأوربي ، كما يمكنه أن يطلب من الوكلاء ذوي الاختصاص الوطني إجراء تحقيقات أو ملاحقات أو التبليغ عن الجرام إلى السلطات المختصة للدول الأطراف. لمزيد من التفصيل انظر :

L'harmonisation des moyens de lutte contre la cybercriminalité ، revue de web، réalisé le 22/4/2004، disponible en ligne à l'adresse suivante: http://www. Finances-gouv.fr

(3) نبيلة هبة مولاي علي هروال، المرجع السابق ، ص 55. لمزيد من التفصيل انظر: د/ شريف السيد كامل، الجريمة المنظمة في القانون، الطبعة الأولى، دار النهضة العربية، القاهرة ، 2001 ، 271 وما بعدها.

(4) نيجل جونز، الاتحاد الأوربي في مجال التدريب على مكافحة الجرائم المعلوماتية، ورقة عمل مقدمة إلى المؤتمر الدولي السادس حول الجريمة المعلوماتية، القاهرة ، من 13 ــ15 أبريل 2005. مشار إليه عند: د/ سليمان احمد فاضل، المرجع السابق، ص 408 وما بعدها .

(5) هذا المكتب هو أحد المكاتب الخمسة التابعة للأمانة العامة لمجلس وزراء الداخلية العرب و مقره دمشق بالجمهورية العربية السورية .

مجال مكافحة الجريمة وملاحقة المجرمين في حدود القوانين و الأنظمة المعمول بها في كل دولة [1] .

2 ـ **على المستوى الداخلي**: بادرت مختلف الدول سواء الأجنبية أو العربية بإنشاء وحدات متخصصة لمكافحة الإجرام الالكتروني على المستوى الوطني، حيث قامت **الولايات المتحدة الأمريكية** بإنشاء إدارة متخصصة لمتابعة الجرائم الالكترونية بمكتب التحقيقات الفدرالي (FBI)[2]، والذي يضم بداخله مجموعة أشخاص مدربين على كيفية متابعة تلك الجرائم والتحري عنها وضبطها والمحافظة على ما يتمّ تحصيله من أدلة .

أما بالنسبة **لفرنسا** لم تسلم هي الأخرى من مخاطر هذا الإجرام [3]، ونتيجة لذلك قرّر وزير الداخلية السابق(Dominique de Villepin) بعد اطلاعه على التقرير المقدّم له من قبل وزير المالية والاقتصاد(Thierry Breton) على ضرورة إتباع مخطط محكم لتحقيق الأمن المعلوماتي، ويتضمّن هذا المخطط ما يلي[4]: ـــ تكوين شبكة خبراء من الشرطة والدرك.

ـــ دعم قوات الشرطة والدرك المتخصصين في مكافحة جرائم الانترنت، وذلك عن طريق زيادة عددهم وتطوير التكوين والتدريب تماشيا مع التطور التكنولوجي الذي يشهده العالم، من خلال عقد مؤتمرات وندوات للانترنت (Forum d'internet) [5] .

---

[1] لمزيد من التفصيل حول المكتب العربي للشرطة الجنائية انظر الموقع التالي :
http://www.websy.com/linker/review.php?sid=15621&recat=226

[2] يشمل البناء التنظيمي لـــ (FBI) على أربعة أقسام رئيسية، هي: القسم الجنائي، قسم الأمن القومي، قسم خدمات التحقيق، وقسم محاربة جرائم الكمبيوتر ومكافحة الإرهاب، ونظرا لزيادة حجم الجرائم الالكترونية أنشأت حكومة الولايات المتحدة الأمريكية في 1998 مركز لحماية الشبكات ويرتبط هذا المركز بجهاز(FBI) وهو متخصص بالرقابة على جميع المواقع الإستراتيجية مثل الدفاع والكهرباء و المياه. كما أنشأت الحكومة الفدرالية سنة 1999 مركز المعلومات من أجل التهديدات المتعلقة بأمن الأنظمة المعلوماتية. كذلك أنشأ مكتب التحقيقات الفدرالي في 2000/5/18 مركز لتلقي شكاوى الاحتيال عبر الانترنت لتلقي البلاغات من خلال موقع المركز على الشبكة الدولية: http://www.ifccb.gov/index.asp. لمزيد من التفصيل انظر موقع مكتب التحقيقات الفدرالي :
. http://www.fbi.gov

[3] جاء في تقرير الجمعية الفرنسية لأمن المعلومات أن الخسائر الناجمة عن الجرائم المعلوماتية قدرت بـــ (10.4) مليار فرنك فرنسي سنة 1991، في سنة 1993 قدرت الخسائر بحوالي (10.8) مليار فرنك فرنسي، وفي سنة 1996 قدرت بحوالي (12.720) مليار فرنك فرنسي . أنظر: د/ نائلة قورة، المرجع السابق، ص 80.

[4] لمزيد من التفصيل انظر: نبيلة هبة مولاي علي هروال، المرجع السابق، ص 40 وما بعدها .

[5] حيث يتم عقد ندوة سنوية مشتركة بالتنسيق بين رجال الشرطة القضائية و رجال الدرك الوطني، تضم هذه الندوة مجموعة من المحققين المتخصصين في مكافحة جرائم الانترنت، من اجل مناقشة الإجرام المعلوماتي ووضع حلول سواء من الناحية النظرية أو التطبيقية .

ـ زيادة الرقابة على المواقع أو تعزيز الرقابة التكنولوجية، فقد تمّ تقسيم هذه المهمة بين رجال الشرطة والدرك، حيث يختص هذا الأخير بالرقابة على المواقع التي تحتوي صورا إباحية، أمّا رجال الشرطة فيختص بمراقبة المواقع التي تبث فيها الجرائم التالية: القرصنة المعلوماتية، الإرهاب والأعمال العنصرية[1].

ـ وفي **هونج كونج** تأسست قوة مكافحة قرصنة الانترنت (The Internet Piracy Hit squad) في ديسمبر1999، حيث تمكنت من القبض على اثني عشر شخصا في خمسة قضايا خلال مدة ستة أشهر من تاريخ إنشاءها[2]، أما في **الصين** فقد تأسست القوة المضادة للهكرة (The anti Piracy institution) في2000/8/22، و التي تتخذ من المعهد العالي للطاقة الفيزيائية مقرا لها، وهي تسعى إلى وضع رقابة شديدة على المعلومات التي يسمح لمواطنيها بالدخول إليها، عن طريق إلزام كل مستخدم شبكة الانترنت بتسجيل نفسه لدى مكاتب الشرطة[3].

أما بالنسبة للدول العربية، وحرصا كغيرها من الدول المتقدمة على مواكبة التطور واللحاق بالمسيرة العلمية من خلال الاعتماد على التقنيات الحديثة، لمواجهة الصور المستحدثة من الإجرام الالكتروني، فقد تم إنشاء إدارة جديدة تختص بمكافحة هذه الجرائم، وهو ما قامت به بالفعل **وزارة الداخلية المصرية** سنة 2002 حيث أنشأت "**إدارة مكافحة جرائم الحاسبات وشبكات المعلومات**"[4] بموجب القرار رقم (13507) وهذه الأخيرة تابعة للإدارة العامة للمعلومات والتوثيق، وتخضع للإشراف المباشر لمدير الإدارة، وتشرف عليها فنيا مصلحة الأمن العام، ويشمل البناء التنظيمي لهذه الإدارة على ثلاث أقسام وهي[5] : قسم العمليات، قسم التأمين و قسم البحوث و المساعدات الفنية، وقد استطاعت أن تضبط العديد من الجرائم التي ارتكبت من خلال شبكة الانترنت: فقد تم ضبط المواقع التي تحتوي على صور و بيانات مخلة بالآداب بتاريخ 2000/12/8، أيضا ضبط جريمة سرقة عبر الانترنت باستخدام كروت الائتمان المملوكة للغير بتاريخ 2/14/ 2001 ، ضبط اختراق لمواقع مكتبة الإسكندرية و تغيير محتواها في 2001/5/30 ...، وتجدر الإشارة إلى أن إدارة مكافحة جرائم الحاسبات

---

(1) La sécurisation du cyberspace،14/4/2005، disponible à l'adresse suivante: http://www.preemier-ministre.gouv.fr .

(2) د / عمر محمد ابوبكر بن يونس، المرجع السابق ، ص 812 .

(3) د / جميل عبد الباقي الصغير، المرجع السابق، ص 77 .

(4) وموقعها الالكتروني هو : http://www.ccd.gov.eg

(5) لمزيد من التفصيل انظر د/ أيمن عبد الحفيظ عبد الحميد سليمان ، المرجـــع الـــسابق، 2003، ص 398 و ما بعدها .

وشبكات المعلومات ليست الإدارة الوحيدة المختصة بمكافحة هذه الجرائم بل هناك عدة جهات تسعى إلى تحقيق هذا الهدف، تتمثل في **الإدارة العامة لمباحث الأموال العامة**[1]، **الإدارة العامة للمصنفات الفنية**[2]، وأخيرا **الإدارة العامة للمعلومات التوثيق**[3].

أمّا بالنسبة **للجزائر** لم يتمّ إلى حدّ الآن إنشاء إدارة متخصصة في مكافحة الجرائم الالكترونية، إلاّ أنّه نظرا لازدياد معدلات الجريمة في الآونة الأخيرة مع ازدياد التقدم العلمي في المجال التكنولوجي واستخدام الجناة للوسائل العلمية الحديثة في ارتكاب جرائمهم، وجد المشرع نفسه مضطرا إلى التدخل من خلال تعديل قانون الإجراءات الجزائية الجزائري وذلك بموجب القانون رقم(06—22) المؤرخ في 29 ذي القعدة عام1427 الموافق لــ(20 ديسمبر 2006)، فاستحدث المشرع فصلين، الرابع والخامس من الباب الثاني من الكتاب الأول، يتمثل الفصل الرابع في" **اعتراض المراسلات وتسجيل الأصوات والتقاط الصور**" حيث أجاز المشرع من خلال المادة (65 مكرر5) لوكيل الجمهورية المختص أن يأذن باعتراض المراسلات التي تتمّ عن طريق وسائل الاتصال السلكية و اللاسلكية.

أما الفصل الخامس فقد جاء تحت عنوان" **في التسرب**" وأجاز فيه المشرع لوكيل الجمهورية أو لقاضي التحقيق بعد إخطار وكيل الجمهورية أن يأذن تحت رقابته بمباشرة عملية التسرب[4]، بمعنى إمكانية ضابط أو عون الشرطة القضائية انتحال هوية مستعارة إذا اقتضت ضرورة التحري أو التحقيق في الجرائم المذكورة في المادة(65 مكرر5) ومن بينها جرائم المساس بأنظمة المعالجة الآلية للمعطيات[5]، وله عند الضرورة القيام بمجموعة من الأفعال المذكورة في المادة (65 مكرر14) منها:

---

(1) تختص هذه الإدارة بمكافحة الجرائم الاقتصادية التقليدية بصفة عامة، و الجرائم المستحدثة بصفة خاصة مثل جرائم تزوير العملات الورقية .

(2) تهتم هذه الإدارة بحماية الملكية الفكرية و حرية الإبداع و التعبير من الأعمال غير المشروعة، كالنسخ و التقليد، حيث تقوم بحملات تفتيشية كبيرة في جميع أنحاء الجمهورية لضبط تلك الجرائم.

(3) تعد من أكثر الإدارات بوزارة الداخلية تعاملا مع الجرائم المعلوماتية، وهي تختص بعملية المتابعة الفنية من خلال التحري عن الجرائم المبلغ عنها من الإدارات الأخرى، كما تقوم بتحديد شخص المتهم من خلال عملية التتبع باستخدام عنوان الانترنت(IP) الذي يتعامل من خلاله الشخص مع شبكة الانترنت . انظر: د/ أيمن عبد الحفيظ عبد الحميد سليمان، المرجع السابق، ص 395 و ما بعدها .

(4) انظر فيما سبق، ص 73 وما بعدها.

(5) تنص الفقرة الأولى من المادة 65 مكرر5 من قانون الإجراءات الجزائية الجزائري: "أذا اقتضت ضرورات التحري في الجريمة المتلبس بها أو التحقيق الابتدائي في جرائم المخدرات أو الجريمة المنظمة العابرة للحدود الوطنية أو **الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات** أو جرائم تبييض الأموال أو الإرهاب أو الجرائم المتعلقة بالتشريع الخاص بالصرف وكذا جرائم الفساد ، يجوز لوكيل الجمهورية المختص أن يأذن بما يلي : ..."

أمّا من حيث التكوين والتأهيل في مجال مكافحة الجرائم الالكترونية فقد قامت الجزائر ببعث إطارات من الدرك الوطني للتكوين والتخصص في البحث والتنقيب، وفي ملاحقة مجرمي المعلوماتية إلى بلدان أجنبية مثل فرنسا والولايات المتحدة الأمريكية "وفق اتفاقيات ثنائية للتعاون

بين البلدين [1]، كما تمّ استحداث شبكة اتصالات وطنية موحدة لجمع البيانات تربط فيما بين مختلف مكاتب الدرك الوطني وتزوّدهم بقاعدة البيانات المتعلقة بشبكات الجريمة المنظمة [2].

---

[1] La gendarmerie étudie les expériences étrangères afin de combattre la cybercriminalité، disponible en ligne à l'adresse suivante :
http://www.algeria.com/forums/computer-internet/21325-cybercriminalit-en-alg-rie-4.html

[2] الجزائر تستعين بالتكنولوجيا الحديثة للتصدي للجريمة المنظمة، مقال منشور في 2008-05-20 على الموقع التالي:
http://www.magharebia.com/cocoon/awi/xhtml1/ar/features/awi/features/2008/05/20/feature-01

المطلب الثاني
الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الالكتروني

إنّ القاضي الجنائي وإن تمتّع بسلطة واسعة في تقديره للأدلة بما في ذلك الدليل الالكتروني، حيث ترك له المشرّع سلطة واسعة، فله أن يتحرّى الحقيقة بكافة الأدلة دون إلزامه بقيمة مسبقة لدليل ما حتى ولو كان دليلا علميّا كالدليل الالكتروني، أو تحديده لنوع معيّن من الأدلة لا يجوز الإثبات بغيرها. ولكن إذا تعمّقنا في دراسة هذه السلطة لا نجدها كما ذهب الفقه السائد[1]، وما استقرّ عليه القضاء[2]، بأنّها **مطلقة وتحكميّة**، بل وضع المشرّع لها ضوابط وهي بمثابة صمام أمان إزاء انحراف القاضي عند ممارسته لها، كي لا تختلّ الأحكام و لا يصار إلى التحكم[3]، إذ أنّ القاضي عليه تسبيب الأحكام .

وعلى ذلك، فإنّ دراستنا للضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الالكتروني نتناولها من جانبين، الأول: يتعلّق بمصدر الاقتناع أي بالدليل الالكتروني الذي يتأسس عليه هذا الاقتناع القضائي، والثاني يتعلق بالاقتناع ذاته، من حيث درجته والسمات المتطلبة فيه، ونخصّص لدراسة كل منهما فرعا مستقلا فيما يلي:

الفرع الأول
الضوابط المتعلقة بمصدر الاقتناع

يمكن القول بأنّ اقتناع القاضي الجنائي بالأدلة الالكترونيّة يحكمه ضابطان، يتمثّل الأوّل في ضرورة أن يتأسّس على دليل الكتروني مقبول، أمّا الثاني، ينبغي أن يكون هذا الاقتناع قائما على أدلة وضعيّة، أي طرحت أمامه في الجلسة في حضور الخصوم.

أولا- شرط مقبوليّة الدليل الالكتروني:

سبق ذكر أنّ القاضي الجنائي ليس حرّا في تقدير الدليل الالكتروني أيّا كان، بل هو حرّ في تقدير **الدليل الالكتروني المقبول** في الدعوى، أي تمّ الحصول عليه بطريق مشروع،

---

(1) د/ محمود مصطفى، شرح قانون الإجراءات الجنائيّة، المرجع السابق، ص 410. وانظر أيضا: محمد زكي أبو عامر، الإجراءات الجنائيّة، المرجع السابق، ص 886. وانظر كذلك: د/ مأمون محمد سلامة، حدود سلطة القاضي الجنائي في تطبيق القانون، دار غريب للطباعة، دار الفكر العربي، القاهرة، 1975، ص 85. د/ رؤوف عبيد، مبادئ الإجراءات الجنائيّة، المرجع السابق، ص 618. د/ احمد فتحي سرور، الوسيط في الإجراءات الجنائيّة، المرجع السابق، ص 500.

(2) حيث قضت محكمة النقض المصريّة أنّ "لقاضي الموضوع في المواد الجنائيّة الحريّة المطلقة في تقدير الوقائع وتكوين اعتقاده منها". نقض فبراير 1923، المعجم الجنائي، ص 217.

(3) د/ فاضل زيدان محمد، المرجع السابق، ص 232.

وبالتالي فإنّ مسألة قبول هذا الدليل ينبغي أن تحظى بالضرورة دراسة سابقة على دراسة حريّة القاضي في تقدير الدليل الالكتروني[1]. لأنّ محل هذه الحريّة هو" الأدلة المقبولة "، وبالتالي فإنّ التطبيق الصرف للقانون يفرض على القاضي أن يكوّن اقتناعه من دليل الكتروني مقبول، ويستبعد في مقابل ذلك من المرافعة سائر الأدلة الالكترونيّة غير المقبولة، لأنّها لا يمكن أن تدخل عنصرا من عناصر تقديره [2].

فمشروعيّة الدليل الالكتروني تعدّ ضمانا كبيرا للحريّة الفرديّة، بل وللعدالة ذاتها، كما أنّها تحمّل القائمين على تجميع أدلة الإدانة على القيام بعملهم بكل نزاهة وذمّة، فليست الإدانة هي الغاية، فالغاية هي تحقيق العدالة والكشف عن الحقيقة، ولا يهدم قرينة البراءة إلاّ الاقتناع اليقيني المبني على أدلّة صحيحة ومشروعة.

ولذلك فلا بد أن يستمد القاضي الجنائي اقتناعه الذاتي في مجال إثبات الجرائم الالكترونيّة من دليل الكتروني مشروع، فلا يجوز الاستناد إلى دليل استمدّ من إجراء باطل وإلا أبطل معه الحكم، فما بني على باطل فهو باطل.

ثانيّا- شرط وضعيّة الدليل الالكتروني:

من القواعد الأساسيّة في الإجراءات الجنائيّة أنّه لا يجوز للقاضي أن يبني حكمه على أدلّة لم تطرح لمناقشة الخصوم في الجلسة، وهو ما يعبّر عنه بوضعيّة الدليل، ومقتضى ذلك أن يكون للدليل أصل ثابت في أوراق الدعوى وأن تتاح للخصوم فرصة الاطلاع عليه ومناقشته، وكلا الأمرين ينبغي توافرهما. وقد أرست هذا الضابط المادة(212 فقرة 2) من قانون الإجراءات الجزائيّة الجزائري إذ تنص :" ولا يسوغ للقاضي أن يبني قراره إلاّ على الأدلة المقدمة له في معرض المرافعات والتي حصلت المناقشة فيها حضوريّا أمامه" [3] .

ونصّت عليها أيضا المادة (302) من قانون الإجراءات الجنائيّة المصري بقولها" ومع ذلك لا يجوز له (أي القاضي) أن يبني حكمه على أيّ دليل لم يطرح أمامه في الجلسة".

---

(1) انظر فيما سبق، ص 136 وما بعدها.

(2) انظر في هذا المعنى، د/ محمد زكي أبو عامر، الإثبات في المواد الجنائيّة، المرجع السابق، ص 139.

(3) كذلك نصت على هذه القاعدة المادة (427) من قانون الإجراءات الجنائيّة الفرنسي في فقرتها الثانيّة بقولها: "لا يجوز للقاضي أن يؤسّس حكمه إلاّ على أدلّة طرحت عليه أثناء المحاكمة ونوقشت أمامه في مواجهة الخصوم".

- Article 427 alinéa 2 du (C.P.P) dispose que :" Le juge ne peut fonder sa décision que sur des preuves [*appréciation*] qui lui sont apportées au cours des débats et contradictoirement discutées devant lui" .

وقد عبّرت محكمة النقض المصريّة عن هذا الضابط بقولها" من المقرر أنّ لمحكمة الموضوع أن تستخلص من جماع الأدلة والعناصر المطروحة أمامها على بساط البحث الصورة الصحيحة لواقعة الدعوى حسبما يؤدي إليه اقتناعها، وأن تطرح ما يخالفها من صور أخرى لم تقتنع بصحتها، ما دام استخلاصها سائغا مستندا إلى أدلّة مقبولة في العقل والمنطق ولها أصل في الأوراق[1].

وعلّة هذه القاعدة هي مبدأ الشفويّة[2] في المحاكمة الجنائيّة، وهو مبدأ أساسي في الإجراءات الجنائيّة، وتقتضيه أولى بديهيات العدالة[3]، حيث يجعل القاضي غير مكتف في تقديره للأدلة سواء كانت تقليدية أو مستخرجة من الوسائل الالكترونية، على ما دوّن بمحاضر التحقيق، وإنّما يتوجّب عليه أن يسمع الشهود واعتراف المتهم بنفسه وما يدلي به الخبراء ويطرح جميع الأدلة الأخرى للمناقشة الشفويّة، فلا يكون هناك وسيط بين الدليل والقاضي. وغاية ذلك حتّى يتاح لكل طرف في الدعوى أن يواجه خصمه بما لديه من أدلة إزاءه ويبيّن موقفه منها، ممّا يفيد القاضي من تكوين قناعته من حصيلة هذه المناقشات التي تجرى أمامه في الجلسة[4].

ولا يختلف الأمر بالنسبة للدليل الالكتروني، سواء كان على شكل بيانات معروضة على شاشة الكمبيوتر، أو مدرجة في حاملات البيانات أو اتخذت شكل أشرطة أو أقراص ممغنطة أو ضوئيّة أو مستخرجة في شكل مطبوعات، كل أولئك سيكون محلا للمناقشة عند الأخذ بها كأدلة إثبات أمام المحكمة[5].

1- عناصر وضعيّة الدليل الالكتروني: يقوم ضابط وضعيّة الدليل الالكتروني على عنصرين أساسيين هما:

أ – إتاحة الفرصة للخصوم للاطلاع على الدليل الالكتروني والرد عليه.

---

(1) نقض رقم 360 السنة 46، جلسة 6/6/ 1976، س 27. وكذلك نقض رقم 929،السنة 53، جلسة 13/10/ 1982. انظر معوض عبد التوّاب ، الوسيط في أحكام النقض الجزائيّة، ص 24 وما بعدها.

(2) إنّ مبدأ الشفويّة في القضاء الجنائي، في أساسه من قواعد النظام الاتهامي والذي ظهرت به الإنسانية منذ الثورة الفرنسية، وقد أقرّته الجمعيّة التأسيسية منذ 18/ 1/ 1791 من نظام الإثبات الجنائي المبني على حريّة القاضي الجنائي في تكوين قناعته، وقد استقرّ النظامان معا، شفويّة المرافعة وقضاء القاضي بمحض اقتناعه، في قانون تحقيق الجنايات الفرنسي الذي صدر في 24 نوفمبر سنة 1808. انظر في ذلك: د/ رؤوف عبيد، المشكلات العمليّة الهامة في الإجراءات الجنائيّة، الجزء الأول، الطبعة الثانيّة، دار الفكر العربي، ص 472.

(3) د/ محمود نجيب حسني، المرجع السابق، ص 427. وانظر أيضا : د/ محمد مروان، المرجع السابق، ص 491.

(4) د/ فاضل زيدان محمد، المرجع السابق، ص 254.

(5) د/ هلالي عبد الله أحمد، حجيّة المخرجات الكمبيوترية في المواد الجنائيّة، المرجع السابق، ص 103.

ب ـ وأن يكون للدليل الالكتروني أصل في أوراق الدعوى.

بالنسبة للعنصر **الأول**، يجب على القاضي مبدئيا أن يطرح كل دليل مقدم في الدعوى للمناقشة أمام الخصوم حتّى يكونوا على بيّنة ممّا يقدّم ضدّهم من أدلة ليتمكّنوا من مواجهة هذه الأدلة والردّ عليها، وذلك احتراما لحقوق الدفاع، الذي يعدّ أحد المظاهر الأساسية لدولة القانون والنظم الديمقراطية[1]، ويتيح مبدأ المواجهة تجسيد هذا الأخير، حيث يقتضي المبدأ الأوّل حضور كل خصم في الدعوى، وأن يطّلع خصمه على ما لديه من أدلة، وأن يواجهه بها، وأن يناقش كل منهما أدلّة الطرف الآخر[2]. ويتطلّب مبدأ المواجهة نوعين من الضمانات:

الأول منها سابق على عمليّة المواجهة ذاتها بين الأطراف في الجلسة، وهو يتضمّن ضرورة إحاطة المتهم علما بالتهمة المنسوبة إليه، وأن يمنح الوقت والوسائل اللازمة لتحضير دفاعه، وأن يسمح له بالاستعانة بمحام للدفاع عنه، وكذلك الاستعانة، عند الاقتضاء بمترجم[3].

أمّا النوع الآخر من الضمانات، فيتمّ أثناء عمليّة المواجهة ذاتها، وهي الأكثر تأثيرا في الدعوى الجنائيّة، إذ يلزم أن يسمح لكل طرف بتقديم ما لديه من مستندات، وسؤال شهود، والخبراء، وأن يطلب اتخاذ أي إجراء يقدر فائدته، وإثارة أي دفوع ، أو إيداع أي مذكرات[4]. ثمّ حق كل طرف في مناقشة أدلة الطرف الآخر وتفنيدها، كسؤال الشهود ومناقشتهم، ومناقشة تقرير الخبير ودحض ما ورد به.

وعلى ذلك، لا يجوز للقاضي الجنائي أن يبني اقتناعه على دليل قدّمه أحد أطراف الدعوى إلا إذا عرض هذا الدليل في جلسة المحاكمة بحيث يعلم به سائر الأطراف. إذ أنّ العدالة تقتضي أن يأتي حكم القاضي بعد مناقشة هادئة ومجادلة حرّة متكافئة من كل صاحب حق مشروع في الدعوى.

أمّا بالنسبة للعنصر **الثاني** والمتمثّل في ضرورة أن يكون للدليل الإلكتروني أصل في أوراق الدعوى، وذلك حتى يكون اقتناع القاضي مبنيّا على أساس، وفي ذلك قالت محكمة النقض المصريّة في حكم حديث لها:" على المحكمة أن تبنى حكمها على الوقائع الثابتة

---

(1) Nicol Opoulos (P)، le procédure devant les juridictions répressives et le principe du contradictoire، revue de science criminel، N' 1 ، 1989، p.3.

(2) د/ محمود نجيب حسني، المرجع السابق، ص 815.

(3) د/ محمد حسن شريف، المرجع السابق، ص 231.

(4) Nicol Opoulos (P)،op.cit، p. 21 et s .

بالدعوى، وليس إقامة قضائها على أمور لا سند لها من التحقيقات" [1]، وأنّ القاضي حرّ في استمداد اقتناعه من أي دليل يطمئن إليه، طالما أنّ له مأخذه الصحيح من الأوراق[2].

ومن أجل ذلك أوجب المشرّع تحرير محضر الجلسة لإثبات وقائع الدعوى الجنائيّة وأدلتها لكي يتمكّن القاضي الموضوع أو أيّ من الخصوم من الرجوع إلى هذا المحضر إذا ما رغبوا في استيضاح أيّ من الوقائع الثابتة به، وذلك منعا للتحكم وتحقيقا للعدالة.

وبالإضافة إلى ذلك، فإنّ هذا التدوين يمكن المحكمة المطعون أمامها، من مراجعة الحكم المطعون فيه وتقديره من حيث الخطأ والصواب[3].

وفي ذلك تشترط محكمة النقض المصريّة أن يكون الدليل الثابت في أوراق الدعوى "عماد الحكم"، أي استندت إليه المحكمة في تكوين عقيدتها[4]، وبخلاف ذلك يكون حكمها معيبا، يستوي في ذلك دليل الإدانة أو البراءة، وذلك لمخالفته لحقوق الدفاع، وهو ما أكّدت عليه محكمة النقض المصريّة في قولها: "إنّه محظور على القاضي أن يبني حكمه على دليل لم يطرح أمامه في الجلسة، يستوي في ذلك أن يكون دليلا على الإدانة أو البراءة، وذلك لكي يتسنى للخصوم الإطلاع عليه والإدلاء برأيهم فيه"[5].

وعبّرت المحكمة عن علّة اقتضاء هذا الشرط بأنّ هذا الدليل قد يكون له من الأثر ما يغيّر وجهة نظر المحكمة، أو أن اطلاع الخصوم على الدليل ومناقشتهم له قد يسفر عن حقيقة قد يتغيّر بها وجه الرأي في الدعوى[6].

2ـ مدى جواز تأسيس اقتناع القاضي الجنائي على علمه الشخصي: من أهمّ النتائج التي تترتب على قاعدة وضعيّة الدليل الالكتروني هي" عدم جواز القاضي أن يقضي استنادا على معلوماته الشخصيّة أو رأي غيره.

ويقصد بالعلم الشخصي للقاضي، معلوماته الشخصيّة التّي يكون قد حصل عليها من خارج نطاق الدعوى المطروحة عليه[7]، والتي من الممكن أن تؤثر في تكوين قناعته عند تقديره لأدلتها.

---

[1] نقض 22 أكتوبر سنة 1990، مجموعة أحكام النقض، س 41،رقم 162، ص 929.
[2] نقض 24 فبراير سنة 1975، مجموعة أحكام النقض، س 26، رقم 42، ص 188.
[3] مأمون سلامة، الإجراءات الجنائيّة، المرجع السابق، ص 170ـــ 175.
[4] نقض 14 أبريل سنة 1952، مجموعة أحكام النقض، س 3، رقم 309، ص 850.
[5] نقض 25 مايو سنة 1982، مجموعة أحكام النقض، س 33، رقم 131، ص 644.
[6] نقض 15 أكتوبر سنة 1973، مجموعة أحكام النقض، س 24، رقم 177، ص 855.
[7] د/ نبيل إسماعيل عمر، قاعدة عدم القضاء بعلم الشخصي للقاضي في الشريعة الإسلاميّة والقانون الوضعي، مجلة الدفاع الاجتماعي، العدد الأول، 1984، ص 41. مشار إليه عند: د/ فاضل زيدان محمد، المرجع السابق، ص 258. وانظر أيضا: د/ محمّد زكي أبو عامر، القيود القضائيّة على حريّة القاضي الجنائي في الاقتناع، ص 46.

فلا يجوز للقاضي أن يبني اقتناعه على هذه المعلومات الشخصيّة، لأنّها من جهة لم تكن موضع مناقشة شفاهيّة بحضور أطراف الدعوى، بل ستكون لهم في الحقيقة مفاجأة إن لم تناقش بمعرفتهم ولم يتمّ إثباتها في إطار إجراءات الخصومة، ممّا يؤدي إلى عدم احترام حقوق الدفاع.

ولأنّ القاضي من جهة ثانية يكون قد جمع في شخصه صفتين متعارضتين صفة الشاهد وصفة القاضي، وهذا ما لا يجيزه القانون ويرتّب عليه بطلان الحكم [1]. ويرجع السبب في ذلك: أنّ من مستلزمات تقدير القاضي الجنائي للأدلة بصفة عامة والدليل الالكتروني على الخصوص، خلو ذهنه من أي معلومات مسبقة بشأنه، فلا تتمّ عمليّة التقدير إلا من خلال طرحه وبيان موقف الخصوم منه، وعندئذ يستطيع القاضي من خلال هذه المناقشة الوصول إلى التقدير السليم. وفي هذا الشأن يقول الفقيه الانجليزي (Sydney Fipson) " ليس للقاضي ولا للمحلف أن يتصرّفا على أساس من علمهما الخاص، بالقضيّة لكن إن كان لديهما وقائع ماديّة يريدان الإدلاء بها فيجب أن يحلفا كشهود فإذا حلفا على هذا النحو فليس للقاضي، بخلاف المحلّف، أن يحكم على أساس من شهادته[2].

أمّا المعلومات العامة المستقاة من خبرة القاضي بالشؤون العامة المفروض إلمام الكافة بها، فهي لا تعدّ من قبيل المعلومات الشخصيّة المحذورة على القاضي أن يبني حكمه عليها، ففي مجال الثقافة المعلوماتية العامة فيما يتعلّق بالمبادئ العامة للكمبيوتر مثل أهم مكونات جهاز الكمبيوتر مثلا.

وتجدر الإشارة في هذا المقام، أنّه ليس للقاضي أن يبني اقتناعه على رأي غيره، إلا إذا كان هذا الغير من الخبراء وقد ارتاح ضميره إلى التقرير المحرّر منه فقرّر الاستناد إليه ضمن باقي الأدلة القائمة في أوراق الدعوى المعروضة عليه، بحيث أنّ الاقتناع الذي يكون أصدر حكمه بناء عليه يكون متولدا من عقيدته هو وليس من تقرير الخبير.

---

[1] جندي عبد الملك، الموسوعة الجنائيّة، دار المؤلفات القانونيّة، الجزء الأول، ص 261. مشار إليه عند: د/ رأفت عبد الفتاح حلاوة، الإثبات الجنائي، قواعده وأدلته، دراسة مقارنة بالشريعة الإسلاميّة، دار النهضة العربيّة، القاهرة، 1996، ص 62.

[2] هذه المقولة مشار إليها: د/ فاضل زيدان محمد، المرجع السابق، ص 260.

الفرع الثاني
الضوابط المتعلّقة بالاقتناع ذاته

يتيح مبدأ الاقتناع القضائي ـ الذي اعتنقه المشرّعان الجزائري والمصري ـ للقاضي الجنائي حريّة كبيرة في تقدير عناصر الإثبات، بما في ذلك الدليل الالكتروني، بل لعلّه أهمّ نتيجة تترتب على هذا المبدأ الهام، لذلك فإنّ تقدير كفاية أو عدم كفاية الدليل الالكتروني في إثبات الجريمة الالكترونيّة ونسبتها إلى فاعلها، أمر تستقلّ به محكمة الموضوع المعروض عليها هذا الدليل، ولا تخضع في ذلك لرقابة محكمة النقض.

غير أنّ ذلك ليس مدعاة إلى القول بأنّ وقائع الدعوى هو ممّا يحظر على محكمة النقض النظر فيها، أو تجاهلها كليّة، وإنّما هي تراقب المنطق القضائي لمحكمة الموضوع بشأن هذه الوقائع، وذلك عن طريق رقابتها لصحّة تسبيب الحكم[1]، لذلك تواترت محكمة النقض على أنّه يلزم لصحّة سلامة اقتناع قاضي الموضوع بالدليل الالكتروني أن يكون مبنيّا على الجزم واليقين، دون الظن والترجيح والاحتمال من ناحيّة، وأن يكون متوائما مع مقتضيات العقل والمنطق من ناحية أخرى.

وبناء على ذلك سوف نعرض للقيود المتعلّقة بالاقتناع ذاته على النحو التالي:

أوّلا: بلوغ الاقتناع القضائي درجة اليقين.

ثانيًا: كون الاقتناع القضائي متوائما مع مقتضيات العقل والمنطق.

أوّلا ـ بلوغ الاقتناع القضائي درجة اليقين:

تهدف الخصومة الجنائيّة إلى معرفة الحقيقة المطلقة، ممّا يقتضي أن يصدر حكم القاضي عن اقتناع يقيني بصحّة ما ينتهي إليه من وقائع، لا بمجرّد الظن والاحتمال، إذ أنّ الشك يفسّر لصالح المتّهم، أخذا بقاعدة أساسيّة أنّ الأصل في الإنسان البراءة، وشرط اليقين في أحكام الإدانة شرط عام سواء كانت الأدلة التي يستقى منها هذا اليقين تقليديّة أو مستحدثة كالدليل الالكتروني.

وبناء على ذلك سوف نتعرض إلى هذا الضابط من خلال أخذ فكرة عامة عن اليقين، ثمّ كيفيّة وصول اقتناع القاضي الجنائي إلى هذا اليقين، ومادام أنّ هذا الأخير شرط حين الحكم بالإدانة، فبمفهوم المخالفة تستثنى حالة البراءة من هذا الشرط، وذلك لأنّ الأصل في الإنسان البراءة حتّى تثبت إدانته، وهو ما سنتعرض له فيما يلي:

---

[1] د/ أحمد فتحي سرور، سلطة محكمة النقض في الرقابة لضمان حسن تطبيق القانون، دار النهضة العربيّة، 1990 ، رقم 16، ص 35.

1ـ فكرة عامة عن اليقين:

إنّ تعريف اليقين في اللّغة هو العلم وزوال الشك وعدم وجود أدنى ريبة[1]. أمّا في الاصطلاح فقد عرّفه الفقهاء بأنّه اعتقاد القاضي بأنّ ما وصل إليه هو الحقيقة[2]. أو هو حالة ذهنيّة وعقليّة تؤكد وجود الحقيقة[3]، والوصول إلى ذلك اليقين يتمّ عن طريق ما تستنتجه وسائل الإدراك المختلفة للقاضي من خلال وقائع الدعوى وما يرتّبه ذلك في ذهنه من تصورات ذات درجة عالية من التوكيد وعندما يصل القارئ إلى هذه المرحلة من اليقين، فإنه يصبح مقتنعا بالحقيقة، فاليقين هو وسيلة الاقتناع أو بعبارة أخرى فإنّ الاقتناع ثمرة اليقين، وليس اليقين ذاته.

2ـ كيفية الوصول إلى اليقين :

يلتزم القاضي أن يبني اقتناعه على سبيل اليقين والجزم، والمطلوب عند الاقتناع ليس اليقين الشخصي للقاضي فحسب، وإنّما هو اليقين القضائي الذي يمكن أن يصل إليه الكافة لاستقامته على أدلة تحمل بذاتها معالم قوّتها في الإقناع [4]، وهو بهذا المفهوم يقوم على عنصرين، أحدهما شخصي، ويلخص في ارتياح ضمير القاضي واطمئنان نفسه إلى إدانة المتّهم على سبيل الجزم واليقين، والثاني موضوعي، ويخلص في ارتكان هذا الارتياح والاطمئنان على أدلّة من شأنها أن تفض لذلك وفقا لمقتضيات العقل والمنطق[5]. بحيث لا يكون عمل القاضي ابتداعا للوقائع وانتزاعا من الخيال[6].

وتكمن العلّة من وراء اقتضاء هذا القيد في أنّ الحكم بإدانة شخص أمر جدّ خطير، وتترتّب عليه آثار جسيمة، ويمكن أن ينال من حريّته أو شرفه أو ماله، بل قد يكون حقّه في

---

(1) مختار الصحاح، المرجع السابق، ص 743.

(2) د/ مفيدة سويدان، المرجع السابق، ص 183.

(3) Rached (A.A), de l'intime conviction du juge, thèse Paris, 1942, p. 3.

مشار إليه عند: د/ هلالي عبد ألاه أحمد، حجيّة مخرجات الكمبيوتريّة في المواد الجنائيّة، المرجع السابق، ص 78.

(4) د/ أحمد فتحي سرور، المرجع السابق، ص475.

(5) د/ محمد عيد غريب، المرجع السابق، ص 130.

(6) نقض 9 يناير سنة 1930، مجموعة القواعد القانونيّة، الجزء الأوّل، رقم 368، ص 416.

الحياة[1]. فضلا عن أنّ القانون قد جعل الأحكام الباتّة عنوانا للحقيقة، لذلك وجب أن تكون تلك الأحكام مبنيّة على الجزم واليقين[2].

وإذا كان القاضي الجنائي يستطيع الوصول إلى اليقين بالأدلة التقليديّة عن طريق المعرفة الحسيّة التي تدركها الحواس، أو المعرفة العقليّة التي يقوم بها القاضي عن طريق التحليل والاستنتاج، فإنّ الجزم بوقوع الجريمة الالكترونيّة ونسبتها إلى المتّهم المعلوماتي تتطلّب نوعا جديدا من المعرفة وهي المعرفة العلميّة للقاضي بالأمور المعلوماتيّة لاسيما وأن القاضي الجنائي يلعب دورا إيجابيّا في الإثبات، وقد يؤدي الجهل في بعض الأحيان إلى التشكك في قيمة الدليل الالكتروني ومن ثمّ يقضي بالبراءة، لاسيما أنّ الشك يستفيد منه المتّهم المعلوماتي في مرحلة المحاكمة، وهذا ما يؤدي إلى إفلات المجرمين من تطبيق القانون.

ويترتب على لزوم بلوغ الاقتناع بالإدانة درجة اليقين أنّه إذا لم يدرك القاضي هذه الدرجة من الاقتناع كان معنى ذلك أنّ اقتناعه يتأرجح بين ثبوت التهمة ومسؤولية المتّهم عنها وبين عدم ثبوتها أو عدم مسؤولية المتّهم عنها، وهذا الاقتناع المتأرجح يعني الشك في ثبوت التهمة . ممّا يستوجب على القاضي أن يحكم بالبراءة.

3 ـ استثناء حالة البراءة من شرط الاقتناع اليقيني:

إذا كان الأصل في الإنسان البراءة، فإنّه يجب لإدانته كما سبق ذكره أن يقوم الدليل القاطع على ارتكابه الجريمة سواء كانت تقليديّة أو مستحدثة كالجريمة الالكترونيّة، بحيث يقتنع القاضي اقتناعا يقينيّا بارتكابها ونسبتها للمتّهم، أمّا فيما يتعلّق الحكم بالبراءة، يكفي أن يتشكّك القاضي في صحّة إسناد التهمة إلى المتّهم حتى يقضي بالبراءة، وذلك إعمالا لمبدأ تفسير الشك لمصلحة المتّهم، وهو ما أكّدته المادة (304)من قانون الإجراءات الجنائيّة المصري، حيث نصّت على أنّه:" إذا كانت الواقعة غير ثابتة، تحكم المحكمة ببراءة المتّهم".

غير أنّ محكمة النقض المصريّة وضعت شرطا لذلك يتمثّل في أنّه يجب أن يتضمّن الحكم ما يفيد أنّ المحكمة قد فحصت الدعوى وأحاطت بأدلّتها عن بصر وبصيرة، ووازنت بين أدلّة الثبوت وأدلّة النفي، ولم تقتنع على وجه اليقين بإدانة المتهم[3]، أو اقتنعت يقينا ببراءته، لأنّه

---

[1] د/ حسن صادق المرصفاوي، المرصفاوي في أصول الإجراءات الجنائيّة، المرجع السابق، ص 624.

[2] د/ السيد محمد حسن شريف، المرجع السابق، ص 364. وانظر أيضا: د/ محمّد علي السالم عياد الحلبي، حريّة القاضي الجنائي في الاقتناع في قوانين مصر والأردن والكويت، مجلة الحقوق، العدد الثالث، السنة الحادية والثلاثون، سبتمبر 2007، الكويت، ص 376.

[3] نقض 10 يناير سنة 1972، مجموعة أحكام النقض، س 23، رقم 17، ص 60. نقض 29 أكتوبر سنة 1990، مجموعة أحكام النقض، س 41، رقم 168، ص 900. نقض 18 ديسمبر سنة 1993، مجموعة أحكام النقض، س 44، رقم 172، ص 1103.

إذا كان من حق محكمة الموضوع أن تستبعد أيّ دليل لا ترتاح إليه، فإنّه لا يجوز لها بتر التحقيق وعدم استكمال عناصره، طالما أنّه منتج ومؤثّر في الدعوى[1].

لذلك قضت محكمة النقض المصريّة بأنه: " ولئن كان من المقرّر أنّ لمحكمة الموضوع أن تقضي بالبراءة متى تشكّكت في صحّة إسناد التهمة إلى المتّهم أو لعدم كفاية أدلة الثبوت، إلاّ أنّ ذلك مشروط بأن يشمل حكمها على ما يفيد أنّها فحصت الدعوى، وأحاطت بظروفها وبأدلة الثبوت التي قام الاتهام عليها عن بصر وبصيرة، ووازنت بينها وبين أدلة النفي فرجّحت دفاع المتّهم، أو داخلتها الريبة في صحّة عناصر الإثبات[2]. وأنّه يكفي في المحاكم الجنائيّة أن يتشكك القاضي في صحّة إسناد التهمة إلى المتّهم، لكي يقضي له بالبراءة، إذ مرجع الأمر في ذلك إلى ما يطمئن إليه في تقدير الدليل ما دام الظاهر من الحكم أنّه أحاط بالدعوى عن بصر وبصيرة [3].

ثانيًا ـ كون الاقتناع القضائي متوائما مع مقتضيات العقل والمنطق:

تواترت محكمة النقض المصريّة على أن يكون استخلاص محكمة الموضوع لواقعة الدعوى استخلاصا معقولا سائغا، ومعيار معقوليّة الاقتناع هو أن يكون الدليل بما في ذلك الدليل الالكتروني مؤديًا إلى ما رتّبه الحكم عليه، من غير تعسّف في الاستنتاج، ولا تنافر مع مقتضيات العقل والمنطق.

وفي ذلك قضت محكمة النقض المصريّة، " أنّه وإن كان من حق محكمة الموضوع أن تستخلص الواقعة من أدلّتها وعناصرها المختلفة، ــ إلاّ أنّ شرط ذلك أن يكون هذا الاستخلاص سائغا تؤدي إليه ظروف الواقعة وأدلتها وقرائن الأحوال فيها .."[4] .

ومع ذلك، تجدر الإشارة إلى أنّ تقييد القاضي الجنائي عند تقديره للدليل الالكتروني بضوابط معيّنة سواء كانت متعلقة بهذا الدليل ذاته أو متعلقة بالاقتناع، غير كافية لضمانة منع الاستبداد والتحكم، بل لابد من ضمانة أخرى أشد من سابقيها، لتجعل سلطة القاضي الجنائي التقديريّة تدور في إطار معتدل بهدف الوصول إلى الحقيقة الواقعيّة باعتبارها غرض الدعوى الجنائيّة، وتتمثّل هذه الوسيلة في رقابة محكمة النقض على سلطة القاضي الجنائي التقديرية.

---

[1] د/ السيد محمد حسن شريف، المرجع السابق، ص 366.

[2] نقض 10 يناير سنة 1972، مجموعة أحكام النقض، س 23، رقم 17، ص 60. نقض 20 فبراير سنة 1972، مجموعة أحكام النقض، س 23، رقم 47، ص 193.

[3] نقض 19 مارس سنة 1975، مجموعة أحكام نقض، س 26، رقم 49، ص 220.

[4] نقض 30 أبريل سنة 1963، مجموعة القواعد القانونيّة، الجزء الرابع، رقم 208، ص 385.

خاتمـــة

بعد أن فرغنا بحمد الله وتوفيقه من دراستنا لموضوع " حجيّة الدليل الالكترونـــي فـــي مجال الإثبات الجنائي"، وقد حاولنا بحث مختلف جوانبه والمشكلات التي أثارها، ينبغي علينا الآن في خاتمة البحث إبراز أهمّ النتائج التّي توصّلنا إليها مع بيان أهمّ المقترحات التّي يرنـــو إليها هذا البحث.

فإذا كان موضوع هذا البحث قد تناول مشكلة مـــن المـــشكلات التـــي أفرزتهـــا ثـــورة المعلومات والاتّصالات عن بعد، فهذه الأخيرة كما نعلم على قدر ما أسعدت البشريّة ويسّرت لها سبل الحياة، فقد أتعستها بهذه النوعيّة الجديدة من الجرائم التي ساهمت هذه الثـــورة فـــي ارتكابها والتي تتميز بطبيعة فنية وعلمية معقدة، ويتصف مرتكبوها بطبيعة ذكية ماكرة.

فلا مرية أن هذه الثورة قد غيّرت الكثير من المفاهيم التقليدية التي كانت تسير دفة الحياة على هديها قبل بزوغ نجمها، فبدأنا نسمع عن العمليات المصرفية الإلكترونية، وعن النقـــود الإلكترونية،وعن المستندات الإلكترونية، وعـــن الحكومـــة الإلكترونيـــة، وعـــن التوقيعـــات الإلكترونية.

ولا شكّ في أنّ ظهور هذه العمليات الجديدة ووجوب حمايتها جنائيا من صور الاعتـــداء المتطورة التي قد تقع عليها بالوسائل الإلكترونية المتطورة، قد أظهر أن هناك قصورا كبيـــرا في النصوص الجنائية الموضوعية، بحيث أنّ هذه النصوص قد أصبحت عاجزة عـــن كفالـــة الحماية الفاعلة للمصالح والقيم التي أفرزتها هذه الثورة.

وإذا كان هذا هو حال التشريعات العقابية الموضوعية، فإن التشريعات الإجرائية لم تكـــن بأسعد حال منها، ولم لا؟ أليست هي الجانب التطبيقي لها.

حيث تبيّن أنّ قصور التشريعات العقابية في مواجهة الجرائم الإلكترونية، قد يترتب عليه وقوع هذه الجرائم، وقد يفلت الجناة من العقاب عنها لعدم وجود نصوص عقابيـــة تجرمهـــا وتعاقب عليها، وهذا القصور سيؤثر على عدم استيفاء الدولة لحقها في العقاب بما سيلحق اشد

الضرر بالمجتمع وأفراده، ويعطل هذا الأمر قانون الإجراءات الجنائية من التطبيق لأنه لم يجد جرائم وعقوبات يتمّ العقاب عنها وفقا لنصوصه، وذلك على الرغم من وقوع هذه الجرائم في الواقع.

فلا يوجد شك في وجود صعوبة كبيرة في إثبات الجرائم الإلكترونية بالنظر إلى طبيعة الدليل الذي يتحصل منها، إذ قد يكون هذا الدليل غير مرئي وقد يسهل إخفائه أو تدميره، وقد يكون متصلا بدول أخرى فتكون هناك صعوبة في الحصول عليه نظرا لتمسك كل دولة بسيادتها. كما أنّ هذا الإثبات قد يحتاج إلى معرفة علمية وفنية قد لا تتوافر لدى رجال الشرطة والمحققين وللقضاة.

وهكذا تحدّدت إشكالية هذا البحث في وجود صعوبة في إثبات الجرائم الإلكترونية، بالنظر إلى الطبيعة الفنية المعقدة لهذه الجرائم واتصاف مرتكبيها بالذكاء والاحتراف، وهو ما حاولنا أن نجتهد في إيجاد الحلول لها وذلك من خلال إلقاء الضوء على طبيعة إثبات هذه الجرائم وطرق الحصول على الأدلة التي تثبتها، ومدى أهميّة الدليل الالكتروني وقيمته في إثبات الجريمة الالكترونيّة.

ولقد توصلنا من خلال هذه الدراسة إلى النتائج الآتية:

1. الدليل الالكتروني عبارة عن معلومات مخزنة في أجهزة الحاسوب وملحقاتها — من دسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات كالطابعات والفاكس — أو متنقلة عبر شبكات الاتصال، والتي يتمّ تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبيها.
2. أهمّ ميزة للدليل الالكتروني تكمن في صعوبة التخلص منه، حيث يمكن استرجاعه بعد محوه، إصلاحه بعد إتلافه، وإظهاره بعد إخفائه.
3. يلزم اتخاذ مسلك الافتراض من حيث اعتبار الدليل الالكتروني دليلا أصليًا، وذلك نتيجة انقص توافر الإمكانات الرقميّة في المحاكم.
4. أظهر البحث كذلك أنّ هناك قصورا واضحا في الكثير من التشريعات الجنائية الإجرائية العربية في مواجهة ظاهرة الجرائم الالكترونيّة، فما زال الكثير منها يُخضِع هذه الجرائم للنصوص التقليدية وهو ما قد يترتب عليه إفلات الكثير من الجناة من العقاب.
5. مواجهة الدول العربيّة للجريمة الالكترونيّة لم يكن على نفس المستوى الموجود في الدول الغربيّة، ففي جمهوريّة مصر العربيّة مثلا لم يصدر تشريعا خاصّا بمكافحة الإجرام الالكتروني حتى الآن، بخلاف الأمر نجده في الجزائر، حيث قامت بتعديل

قانونها العقابي بموجب القانون رقم (04 ـــ 15) المؤرخ في العاشر من نوفمبر عام 2004، فقامت بإضافة قسم خاص بهذا النوع المستحدث من الإجرام تحت عنوان " **المساس بأنظمة المعالجة الآلية للمعطيات**"، وقد صاحب هذا التعديل، تعديل في قانون الإجراءات الجزائيّة الجزائري بموجب القانون رقم (06 ـــ 22) المؤرخ في 20 ديسمبر 2006، وذلك بشأن ملاحقة هذه الجرائم.

6. أظهر البحث كذلك أن هناك صعوبة تكتنف الدليل الإلكتروني سواء من حيث طرق الحصول عليه أو من حيث طبيعته. فالحصول عليه قد يحتاج إلى عمليات فنية وعلمية وحسابية معقدة. كما وأنّ طبيعته قد تكون غير مرئية، كالذبذبات والنبضات، وأنه من السهولة استخدام التقنية العلمية في إخفائه أو إتلافه وقد يتم ذلك طريق التشفير وكلمات المرور السرية واستخدام الفيروسات المدمرة أو التالفة.
7. أصبح من المقرّر في التشريعات المختلفة أنّه يجوز التفتيش لضبط المعلومات على الرغم من طبيعتها المعنويّة.
8. يجوز أن يصدر إذن التفتيش مقتصرا على تفتيش الكمبيوتر، فإذا كان هذا الأخير متواجدا في أحد المساكن، يتعيّن توافر شروط تفتيش المساكن (صدور إذن قضائي مسبّب)، أما إذا كان الكمبيوتر في حيازة الشخص خارج مسكنه أو كان في سيارته خارج المسكن، فإنّه يكفي توافر شروط تفتيش الشخص.
9. استحدث المشرّع الجزائري إجراء التسرّب كوسيلة لمواجهة جرائم المساس بأنظمة المعالجة الآليّة للمعطيات.
10. لا يمكن إلزام الشاهد بالإدلاء بما لديه من معلومات لازمة لولوج نظام المعالجة الآليّة للبيانات تنقيبا عن أدلة الجريمة الالكترونيّة.
11. أظهر البحث كذلك أن هناك قصورا في التشريعات الإجرائية، فما زال الكثير منها يقف في حمايته للحريات الشخصية وحرمة الحياة الخاصة من الوسائل الإلكترونية عند النصوص التقليدية التي تنص – فقط – على حماية هذه الحريات من وسائل الاتصال التقليدية.
12. كما تبيّن أيضا من البحث أنّ الشخص يتمتّع بالحق في الخصوصيّة على بريده الالكتروني، فلا يجوز الإطلاع عليه أو اعتراضه بدون رضاء صاحبه، إلاّ بشروط يجب أن يحدّدها القانون مستهديا بما يحدث بالنسبة للبريد العادي.
13. لا تكتف الإجراءات التقليدية لجمع الدليل الالكتروني، بل لابدّ وان تصاحبها إجراءات حديثة تتّفق مع الطبيعة العلميّة والتقنيّة للدليل الالكتروني كالتحفظ المعجّل على

البيانات المعلوماتيّة، الأمر بتقديم بيانات معلوماتيّة خاصة بالمشترك و اعتراض الاتصالات الالكترونيّة.

14. تضع بعض التشريعات المقارنة كالقانون الفرنسي التزاما على مزودي الخدمات بإزالة البيانات التي يتمّ تخزينها تلقائيًا وتتعلّق بالاتصالات الالكترونيّة بين مستعملي شبكة الانترنت وتسمح بمعرفة هويّة المتّصلين وساعة الاتصال.

15. حرصت كافة التشريعات المختلفة على مبدأ مشروعية الدليل الالكتروني.

16. يعتبر مبدأ حرية الإثبات الجنائي أساس قبول الدليل الالكتروني في الإثبات الجنائي، عند الدول ذات الأصل اللاتيني، وغيرها من الدول المتأثرة بها كالجزائر ومصر.

17. ألقى البحث الضوء على كل من الحقيقة العلمية والحقيقة القضائية وانتهى إلى أن الحقيقة العلمية قد تشوش وتضلل الحقيقة القضائية، وهو ما يلقي مزيدا من الأهمية لتدريب الخبراء والمحققين والقضاة لأجل فهم هذه الحقيقة العلمية والعمل على مطابقة الحقيقة القضائية لها على قدر المستطاع.

18. أظهر البحث أنّ الإثبات الجنائي مهما تطوّر بالنسبة للجرائم الإلكترونية وعلا شأن الأدلة العلميّة والفنيّة، في هذا الإثبات، فإنّه يجب أن نبقى على سلطة القاضي التقديريّة في تقديره لهذه الأدلة العلمية والفنية، لأنّنا بذلك نضمن تنقية هذه الأدلة من شوائب الحقيقة العلمية، ويظل القاضي هو المسيطر على هذه الحقيقة لأنه من خلال سلطته التقديرية يستطيع أن يفسّر الشك لصالح المتّهم، وأن يستبعد الأدلة الالكترونيّة التي يتمّ الحصول عليها بطرق غير مشروعة.

19. أظهر البحث أيضا تأثر قانون الإجراءات الجنائية بقانون العقوبات بالنسبة لإثبات المسائل غير الجنائية التي تدخل عناصر تكوينية في بعض الجرائم، ذلك أن هذه المسائل قد تغير مضمونها، فقد ظهرت الشيكات الإلكترونية، والمحررات الإلكترونية، ولذلك فإن إثبات هذه المسائل سيكون بالأدلة التي تتفق مع طبيعتها والتي تجد مصدرها في قوانين غير عقابية كالقانون التجاري والقانون المدني.

على ضوء هذه النتائج فإن البحث قد توصل إلى المقترحات الآتية:

1. يجب تعديل النصوص الإجرائية التي نصت على حماية حرمة الحياة الخاصة من الرقابة عليها بوسائل الاتصالات السلكية واللاسلكية إلا وفقا للقيود والضوابط المنصوص عليها في هذه النصوص، بحيث أن تشمل هذه الحماية أي وسيلة من وسائل الاتصال لكي نحمي الأسرار الخاصة للأفراد من الوسائل الإلكترونية المستجدة.

2. دعوة المشرّع الجزائري إلى إضافة عبارة "**المعطيات المعلوماتية**" في المادة (81) من قانون الإجراءات الجزائيّة الجزائري لتصبح المادة على النحو التالي:" يباشر التفتيش في جميع الأماكن التّي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة".

3. يجب الاهتمام بتدريب الخبراء والمحققين والقضاة على التعامل مع الجرائم الإلكترونية ذات الطبيعة الفنية والعلمية المعقدة، بحيث يمكن الوصول إلى الحقيقة وإماطة اللثام عن هذه الجرائم تحقيقا لصالح المجتمع وأفراده، ولصالح المتهمين أنفسهم لكي لا يدان إلا المسيء ويبرأ البريء.

4. يجب أن تعد الدول العربية العدة لمواجهة الظاهر الإجرامية المستجدة التي من المنتظر أن تتزايد في المستقبل كنتيجة للتطور العلمي المستمر الذي أحدثته ثورة الاتصال عن بعد، بحيث تجني ثمار هذه الثورة، ولا تقف عند السير على أشواكها، فإنه قد يكون من العجب ونحن مهد الحضارة أن نبدأ من حيث انتهى الآخرون، وإنما يجب علينا أن نساير ركب التقدم العلمي في مختلف مناحي الحياة، سواء تعلق ذلك بالنواحي الاقتصادية أم بالنواحي السياسية أم بالنواحي الثقافية، أم بالنواحي التشريعية.

5. ضرورة التعاون الدولي لمواجهة الجرائم الالكترونيّة، وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرّم صور هذه الجرائم كلّها، وتبين كيفية تسليم مجرمي المعلوماتية، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بهذا النوع من الإجرام.

6. دراسة اتفاقية بودابست لمواجهة الجريمة الالكترونيّة، ودراسة إمكانيّة الانضمام إليها للاستفادة ممّا تتيحه هذه الاتفاقية من تسهيلات في مكافحة هذا النوع المستحدث من الإجرام.

7. تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشأ منها في كليات الحقوق والمعاهد القضائيّة وكذلك في كليّات الشرطة.

8. وأخيرا نهيب بالمشرع الجزائري والمصري تعديل قانون الإجراءات الجنائيّة وذلك بإضافة المواد التالية:

ـ لا يجوز اعتراض أو تسجيل الرسائل الالكترونيّة أو المحادثات الالكترونيّة الفوريّة بين المتّهم والمدافع عنه إلاّ في الأحوال التي يبيّنها القانون.

ـ إذا صدر إذن بتفتيش نظام معيّن لمعالجة المعلومات آليّا للحصول على دليل يفيد في كشف الحقيقة عن جريمة معيّنة، جاز تفتيش كلّ الملفات المتواجدة في النظام.

ـ يجوز ضبط البيانات المتواجدة في نظام معالجة آليًا بدون ضبط النظام نفسه، وذلك بأخذ نسخة من البيانات الموجودة، ويلتزم المحقق بالتحفظ عليها بشكل يمنع أن تمتد يد العبث إليها.

وهكذا يكون البحث قد اكتملت عناصره، فإن كان فيه كمال فهو لله سبحانه وتعالى، وإن اعتراه النقص فهو مني، ولم لا وأنا بشر أجتهد فأخطئ وأصيب، فإن أصبت فأجري على الله وإن أخطأت فأدعوه ألا يحرمني أجر المجتهدين.

وأسأل الله أن يهدينا إلى سواء السبيل، وأن يجعل عملي هذا خالصا لوجهه الكريم، وأن ينفع به، إنّه نعم المولى ونعم النصير، وآخر دعوانا أن الحمد لله رب العالمين.



قائمة المراجع:

أوّلا : المؤلفات باللغة العربيّة

أ ـ المؤلفات العامة:

- د/ أحمد شوقي الشلقاني، مبادئ الإجراءات الجزائية في التشريع الجزائري، ديوان المطبوعات الجامعية، الجزائر ، 1999 .
- د/ أحمد فتحي سرور، الوسيط في قانون الإجراءات الجنائية، دار النهضة العربيّة، القاهرة، الطبعة الثانيّة،1981.
- د/ أحمد فتحي سرور، أصول الإجراءات الجنائيّة، دار النهضة العربية، القاهرة، 1969.
- د/ أحمد عوض بلال، الإجراءات الجنائيّة المقارنة، والنظام الإجرائي في المملكة العربيّة السعوديّة، دار النهضة العربيّة، القاهرة، 1991.
- د/ جلال ثروت, نظم الإجراءات الجنائيّة, دار الجامعة الجديدة للنشر, الاسكندرية, 1997.
- د/ حسن صادق المرصفاوي، أصول الإجراءات الجنائية في القانون المقارن، منشأة المعارف الإسكندرية، 1982.
- د/ رؤوف عبيد، مبادئ الإجراءات الجنائيّة في القانون المصري، دار الفكر العربي، 2006.
- د/ رؤوف عبيد، المشكلات العمليّة الهامة في الإجراءات الجنائيّة، الجزء الأول، الطبعة الثانيّة، دار الفكر العربي.
- د/ رمسيس بهنام، المحاكمة والطعن في الأحكام، منشأة المعارف، 1993.
- د/ سليمان مرقس، أصول الإثبات وإجراءاته في المواد المدنيّة في القانون المصري مقارنا بتقنينات سائر البلاد العربيّة، الطبعة الرابعة ، دار النهضة العربيّة، 1986.
- د/ عوض محمد عوض:
  - قانون الإجراءات الجنائي، الجزء الأول، مؤسسة الثقافة الجامعية، 1989.
  - د/ عوض محمد عوض، التفتيش في ضوء أحكام النقض، دراسة مقارنة، بدون دار النشر، الإسكندرية، 2006.

- د/ قدري عبد الفتاح الشهاوي، ضوابط التفتيش في التشريع المصري والمقارن، منشأة المعارف، الإسكندرية، 2005.
- د/ مأمون محمد سلامة:
  - الإجراءات الجنائية في التشريع المصري، دار النهضة العربية ، القاهرة، 2000.
  - قانون الإجراءات الجنائية معلقا عليه بالفقه وأحكام النقض، الجزء الثاني، الطبعة الثانية، 2005، بدون دار النشر.
- د/ محمد زكي أبو عامر:
  - الإثبات في المواد الجنائيّة، الفنيّ للطباعة والنشر، الإسكندرية، بدون تاريخ النشر.
  - د/ محمد زكي أبو عامر، الإجراءات الجنائيّة، دار الجامعة الجديدة، الإسكندرية، الطبعة السابعة، 2002.
- د/ محمود محمود مصطفى:
  - الإثبات في المواد الجنائية في القانون المقارن، الجزء الأول، النظرية العامة، مطبعة جامعة القاهرة والكتاب الجامعي، الطبعة الأولى، 1977.
  - شرح قانون الإجراءات الجنائيّة، مطبعة دار النشر الثقافة، الطبعة الثانية القاهرة، 1953.
  - الإثبات في المواد الجنائية في القانون المقارن، الجزء الثاني، التفتيش و الضبط، الطبعة الأولى، مطبعة جامعة القاهرة، 1978.
- د/ محمد محي الدين عوض، الإثبات بين الازدواج والوحدة، مطبوعات جامعة القاهرة بالخرطوم، 1974.
- د/ محمود نجيب حسني، شرح قانون الإجراءات الجنائية، الطبعة الثانية، دار النهضة العربة، القاهرة، 1988.

ب ـ المؤلفات الخاصة:

- د/ أحمد حسام طه تمام، الحماية الجنائيّة لتكنولوجيا الاتصالات، دراسة مقارنة، دار النهضة العربيّة، 2002.
- د/ أحمد خليفة الملط ، الجرائم المعلوماتية ــ دراسة مقارنة ــ دار الفكر الجامعي ، 2005 .

- د/ أحمد عوض بلال، اعدة استبعاد الأدلة المتحصلة بطرق غير مشروعة في الإجراءات الجنائيّة المقارنة، الطبعة الثانية، دار النهضة العربية، القاهرة، 2006.
- د/ أحمد فتحي سرور، سلطة محكمة النقض في الرقابة لضمان حسن تطبيق القانون، دار النهضة العربيّة، 1990.
- د/ أسامة أحمد المناعسة، جلال محمد الزغبي وفاضل الهواوشة، جرائم الحاسب الآلي والانترنت، دار وائل للنشر، عمان، الطبعة الأولى، 2001.
- أمير فرج يوسف، الجرائم المعلوماتية على شبكة الانترنت، دار المطبوعات الجامعية، إسكندرية ،2008 .
- أمين الرومي، جرائم الكمبيوتر والأموال، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003.
- د/ أمين مصطفى محمّد:
  - الحماية الجنائيّة الإجرائيّة للصحفي, دراسة في القانونين المصري والفرنسي, دار النهضة العربيّة, القاهرة, 2008.
  - حماية الشهود في قانون الإجراءات الجنائيّة, دراسة مقارنة, دار النهضة العربيّة, القاهرة، 2008.
- د/ برهامي أبوبكر عزمي، الشرعيّة الإجرائيّة للأدلة العلميّة، دراسة تحليليّة لأعمال الخبرة، دار النهضة العربيّة ، القاهرة، 2006 .
- بيل جيتس، المعلوماتية بعد الانترنت، طريق المستقبل، ترجمة عبد السلام رضوان، الكويت، المجلس الوطني للثقافة والفنون والآداب، 1998.
- د/ جميل عبد الباقي الصغير:
  - أدلة الإثبات الجنائي والتكنولوجيا الحديثة، دراسة مقارنة، دار النهضة العربية، القاهرة، 2002.
  - الانترنت والقانون الجنائي، الأحكام الموضوعيّة للجرائم المتعلّقة بالانترنت، الطبعة الأولى، دار النهضة العربيّة، 2001.
  - الجوانب الإجرائية للجرائم المتعلقة بالانترنت، دار الفكر العربي، القاهرة، 2001.
- حسن طاهر داود "جرائم نظم المعلومات" الإصدار رقم 244, لأكاديمية نايف العربية للعلوم الأمنية – الرياض – السعودية ، 2000.

- د/ خالد حمد محمد الحمادي، الثورة البيولوجية و دورها في الكشف عن الجريمة DNA، دار الجامعة الجديدة، 2005.
- د/ خالد مصطفى فهمي، الحماية القانونية لبرامج الحاسب الآلي في ضوء قانون حماية الملكية الفكرية المصري ، رقم 82 لسنة 2002 ، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية, 2005، ص 36.
- د/ رأفت عبد الفتاح حلاوة، الإثبات الجنائي، قواعده وأدلته، دراسة مقارنة بالشريعة الإسلاميّة، دار النهضة العربيّة، القاهرة، 1996.
- رامي عبد العزيز، الفيروسات وبرامج التجسس، دار البراءة ، الإسكندرية ، 2005.
- د/ رمزي رياض عوض، حماية المتّهم في النظام الأنجلوأمريكي، دار النهضة العربيّة، القاهرة، 1998.
- سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الانترنت، دار الفكر الجامعي، 2007 .
- سراج الدين الروبي، الانتربول وملاحقة المجرمين ، دار المصرية اللبنانية، 1998 .
- د/ سعد أحمد محمود سلامة، مسرح الجريمة، الطبعة الأولى، دار النهضة العربية، القاهرة، 2007.
- د/ سعيد عبد اللطيف حسن، إثبات جرائم الكمبيوتر والجرائم المرتكبة عبر الانترنت، الطبعة الأولى ، دار النهضة العربية، القاهرة ، 1999.
- د/ سليمان أحمد فاضل، المواجهة التشريعيّة والأمنيّة للجرائم الناشئة عن استخدام شبكة المعلومات الدولية (الانترنت)، دار النهضة العربية، القاهرة، 2007.
- د/ شريف السيد كامل، الجريمة المنظمة في القانون، الطبعة الأولى، دار النهضة العربية، القاهرة، 2001.
- د/ طارق سرور، حق المجني عليه في تسجيل المحادثات التليفونيّة الماسة بشخصه، دار النهضة العربيّة، الطبعة الثانيّة، 2004.
- د/ عبد الحكم فوده، حجية الدليل الفني في المواد الجنائية و المدنية ـــ دراسة علمية على ضوء قضاء النقض ـــ دار الألفي لتوزيع الكتب القانونية بالمنيا ، بدون تاريخ الطبع.
- د/ عبد العظيم وزير، شرح قانون العقوبات ـــ القسم الخاص ـــ جرائم الاعتداء على الأموال، الطبعة الأولى، دار النهضة العربية، القاهرة، 1993.

- د/ عبد الفتاح بيومي حجازي:
  - الأحداث والانترنت، دار الفكر الجامعي، الإسكندرية، 2004.
  - الدليل الجنائي والتزوير في جرائم الكمبيوتر والانترنت ـ دراسة متعمقة في جرائم الحاسب الآلي الانترنت ـ دار الكتب القانونية، مصر، المحلة الكبرى، 2002.
  - مبادئ الإجراءات الجنائية في جرائم الكمبيوتر والانترنت، دار الفكر الجامعي، الطبعة الأولى، 2006، الإسكندرية.
  - التوقيع الالكتروني في النظم القانونيّة المقارنة، دار الفكر الجامعي، الطبعة الأولى، 2005.
- عبد الفتاح سليمان، مكافحة غسيل الأموال، دار علاء الدين، القاهرة، الطبعة الأولى، 2004.
- د/ عبد الله حسين محمود، سرقة المعلومات المخزنة في الحاسب الآلي، الطبعة الثانية، دار النهضة العربية ،القاهرة، 2002.
- د/ عفيفي كامل عفيفي، جرائم الكمبيوتر وحقوق المؤلف والمصنّفات الفنيّة، ودور الشرطة والقانون، دراسة مقارنة، بدون تاريخ ودار النشر.
- د/ علاء الدين محمد فهمي وآخرون ، د/.محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الإلكتروني، القاهرة مطابع المكتب المصري الحديث ،1991.
- د/ علي بن هادي البشري، الجهود القانونيّة للحد من من جرائم الحاسب الآلي، مكتبة ملك فهد الوطنيّة، الطبعة الأولى، الرياض، 2005.
- د/ علي عبد القادر القهوجي، الحماية الجنائيّة لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر، 1997.
- د/ عماد عوض عدس، التحريّات كإجراء من إجراءات البحث عن الحقيقة، دار النهضة العربيّة، القاهرة، 2007.
- د/ عمر محمد بن يونس، الإجراءات الجنائية عبر الانترنت، المرشد الفدرالي الأمريكي لتفتيش و ضبط الحواسيب وصولا إلى الدليل الالكتروني في التحقيقات الجنائية، بدون دار النشر، 2006 .
- د/ عمر بن يوسف و د/ يوسف أمين شاكير،غسل الأموال عبر الانترنت، الطبعة الأولى، أقاسوس، القاهرة ،2004.

- د/ مأمون محمد سلامة، حدود سلطة القاضي الجنائي في تطبيق القانون، دار غريب للطباعة، دار الفكر العربي، القاهرة، 1975.
- د/ محمد أبو العلاء عقيدة، مراقبة المحادثات التلفونيّة، دراسة مقارنة، دار الفكر العربي، 1994.
- محمد أحمد غانم، الجوانب القانونيّة والشرعيّة للإثبات الجنائي بالشفرة الوراثيّة، دار الجامعة الجديدة، 2008.
- د/ محمد حماد مرهج الهيتي، التكنولوجيا الحديثة والقانون الجنائي، دار الثقافة للنشر والتوزيع،2004.
- د/ محمد سامي الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات، دار النهضة العربية، القاهرة، 1998.
- محمد علي العريان، عمليات غسل الأموال و آليات مكافحتها ــ دراسة مقارنة ــ دار الجامعة الجديدة للنشر، الإسكندرية، 2005.
- د/ محمد عيد الغريب، حريّة القاضي الجنائي في الاقتناع اليقيني وأثره في تسبيب الأحكام الجنائيّة، النسر الذهبي للطباعة، 1996ــ 1997.
- د/ محمد الأمين البشري، التحقيق في الجرائم المستحدثة، الطبعة الأولى، جامعة نايف العربية للعلوم الأمنية، الرياض ، 2004.
- د/ محمد فهمي، الموسوعة الشاملة لمصطلحات الحاسب الالكتروني، مطابع المكتب المصري الحديث، القاهرة، بدون تاريخ نشر.
- محمد محمد شتا، فكرة الحماية الجنائية لبرامج الحاسب الآلي، دار الجامعة الجديدة للنشر،2002.
- د/ محمد محمد محمد عنب، موسوعة العلوم الجنائية، تقنية الحصول على الآثار والأدلة المادية، الجزء الأول، مركز بحوث الشرطة، الشارقة، الطبعة الأولى، 2007.
- محمود عبد الرحيم الديب, الحماية القانونية للملكية الفكرية, في مجال الحاسب الآلي والانترنت, دار الجامعة الجديدة للنشر, 2005 , ص 28 و ما بعدها.
- د/ مصطفى محمد موسى، أساليب إجرامية بالتقنية الرقمية ماهيتها ..مكافحتها ، دراسة مقارنة، مطابع الشرطة، الطبعة الأولى ، 1423 هــ ــ 2003 .
- د/ معجب معدي الحويقل، دور الأثر المادي في الإثبات الجنائي، أكاديمية نايف العربية للعلوم الأمنية ،الطبعة الأولى ، الرياض.

- د/ ممدوح عبد الحميد عبد المطلب، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر و الانترنت، دار الكتب القانونية، مصر، المحلة الكبرى ، 2006 .
- منير محمد الجنبيهي، ممدوح محمد الجنبيهي، جرائم الانترنت، دار الفكر الجامعي، الإسكندرية، 2004.
- مولاي ملياني بغدادي، الخبرة القضائيّة في المواد المدنيّة، مطبعة حلب، الجزائر، 1992.
- د/ نادر عبد العزيز شافي، المصارف والنقود الالكترونيّة، الطبعة الأولى، المؤسسة الحديثة للكتاب، لبنان، طرابلس، 2007.
- نهلا عبد القادر المومني، الجرائم المعلوماتيّة، دار الثقافة للنشر والتوزيع، الطبعة الأولى، 2008.
- د/ هدى حامد قشقوش، الحماية الجنائيّة للتجارة الالكترونيّة، دار النهضة العربيّة ، القاهرة.
- د/ هشام محمد فريد رستم:
  - قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، أسيوط، 1992.
  - الجوانب الإجرائية للجرائم المعلوماتية، دراسة مقارنة، مكتبة الآلات الحديثة، أسيوط، 1994.
- د/ هلالي عبد الله أحمد:
  - الجوانب الموضوعية والإجرائية لجرائم المعلوماتية على ضوء اتفاقية بودابست الموقعة في 23 نوفمبر 2001، الطبعة الأولى، دار النهضة العربية، القاهرة، 2003.
  - تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي، دراسة مقارنة، دار النهضة العربيّة ، القاهرة، 2006.
  - التزام الشاهد بالإعلام في الجريمة المعلوماتية، دراسة مقارنة، دار النهضة العربية، القاهرة، 2006.
  - حجيّة المخرجات الكمبيوترية في المواد الجنائيّة، دراسة مقارنة، الطبعة الأولى، دار النهضة العربيّة، 1997.

ج ـ الرسائل العلميّة:

– د/ إبراهيم الغماز، الشهادة كدليل إثبات في المواد الجنائية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1980.

– د/ إبراهيم محمد إبراهيم محمّد، النظريّة العامة لتفتيش المساكن في قانون الإجراءات الجنائيّة، دراسة مقارنة، رسالة دكتوراه ، كليّة الحقوق، جامعة القاهرة، 2005.

– د/ أحمد أبو القاسم، الدليل المادي ودوره في الإثبات في الفقه الجنائي الإسلامي ـــ دراسة مقارنة ـــ دار النهضة العربية، 1991.

– د/ أحمد حسام طه تمام، الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، الطبعة الأولى، دار النهضة العربية ، القاهرة ، 2000.

– د/ أحمد ضياء الدين محمد خليل، مشروعيّة الدليل في المواد الجنائيّة، دراسة تحليلية مقارنة لنظريتي الإثبات والمشروعيّة في مجال الإجراءات الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامع عين شمس، 1982.

– د/ أحمد فتحي سرور، نظريّة البطلان في قانون الإجراءات الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1959.

– د/ السيد محمّد حسن شريف، النظريّة العامة للإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 2002.

– د/ أمال عثمان، الخبرة في المسألة الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1964.

– د/ أمين أعزان، الحماية الجنائية للتجارة الالكترونية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007.

– د/ أيمن عبد الحفيظ عبد الحميد سليمان، إستراتيجية مكافحة الجرائم الناشئة عن استخدام الحاسب الآلي، دراسة مقارنة، رسالة دكتوراه، أكاديميّة الشرطة 2003.

– د/ أيمن فاروق عبد المعبود حمد، الإثبات الجنائي بشهادة الشهود في الفقه الجنائي الإسلامي و القانون الجنائي الوضعي، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2004.

– د/ سامي حسن الحسني، النظرية العامة للتفتيش في القانون المصري والمقارن، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 1996.

- د/ سيف الغافري، السياسة الجنائية في مواجهة جرائم الانترنت، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة.

- د/ شيماء عبد الغني محمد عطا الله، الحماية الجنائية للتعاملات الالكترونية، دار الجامعة الجديدة ،2007.

- د/ عبد الخالق محمّد أحمد ثابت الصلوي، حجيّة الخبرة الجنائيّة، دراسة مقارنة، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، 2008.

- د/ عبد الوهاب العشماوي، الاتهام الفردي أو حق الفرد في الخصومة الجنائيّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1953.

- د/ عمر محمد أبوبكر بن يونس، الجرائم الناشئة عن استخدام الانترنت، رسالة دكتوراه، جامعة عين شمس، 2004.

- د/ فاضل زيدان محمّد، سلطة القاضي الجنائي في تقدير الأدلّة، دراسة مقارنة، رسالة دكتوراه، كليّة الحقوق، جامعة بغداد، 1992.

- د/ فتحي محمد أنور محمد عزت، دور الخبرة في الإثبات الجنائي، دراسة مقارنة، رسالة دكتوراه، كليّة الحقوق، جامعة عين شمس، 2007.

- د/ فرج إبراهيم العدوي عبده، سلطة القاضي الجنائي في تقدير الأدلّة، رسالة دكتوراه، كليّة الحقوق، جامعة القاهرة، 1995.

- محمد بن نصير محمد السرحاني، مهارات التحقيق الفني في جرائم الحاسوب والانترنت، دراسة مسحية على ضباط الشرطة بالمنطقة الشرقية في العلوم الشرطية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، سنة 2004.

- د/ محمد محمد محمد عنب، معاينة مسرح الجريمة، رسالة دكتورا، كلية الدراسات العليا، أكاديمية الشرطة، 1988.

- د/ محمد مروان، وسائل الإثبات في المواد الجنائيّة في القانون الوضعي والجزائري، الجزء الثاني، ديوان المطبوعات الجامعيّة، الجزائر، 1998.

- د/ مفيدة سويدان، نظريّة الاقتناع الذاتي للقاضي الجنائي، دكتوراه كليّة الحقوق، جامعة القاهرة، 1985.

- محمد مسعود خليفة, الحماية الجنائيّة لمعطيات الحاسب الآلي في القانون الجزائري والمقارن, رسالة ماجستير, كليّة الحقوق, جامعة الاسكندريّة, 2005ـ 2006.

- د/ نائلة عادل محمد فريد قورة، جرائم الحاسب الآلي الاقتصاديّة، دراسة نظرية وتطبيقية، منشورات الحلبي الحقوقيّة، 2005.

- نبيلة هبة مولاي علي هروال، الجوانب الإجرائية لجرائم الانترنت في مرحلة جمع الاستدلالات، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الإسكندرية، 2005 – 2006.

- د/ هبة أحمد علي حسانين، الحماية الجنائية لحرمة الحياة الخاصة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2007.

- د/ هلالي عبد الله أحمد، النظرية العامة للإثبات في المواد الجنائية ـ دراسة مقارنة بالشريعة الإسلامية ـ رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، سنة 1984.

- د/ ياسر الأمير فاروق محمد، مراقبة الأحاديث الخاصة في الإجراءات الجنائيّة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، 2008.

د ـ المقالات:

- د/ أحمد أبو القاسم:
  - المفهوم العلمي والتطبيقي للدليل الجنائي المادي، مجلة مركز بحوث الشرطة، العدد السابع والعشرون، يناير، 2005.
  - الدليل الجنائي المادي ودوره في إثبات جرائم الحدود والقصاص، بحث منشور في بالمركز العربي للدراسات الأمنية والتدريب بالرياض، 1993.

- د/ أمين مصطفى محمد, الحماية الجنائيّة لحقوق الملكيّة الصناعيّة في ضوء الاتفاقيات الدولية والقوانين الوطنيّة, مجلة الحقوق للبحوث القانونيّة والاقتصاديّة, العدد الثاني, 2007.

- د/ أيمن عبد الحفيظ، حدود مشروعية دور أجهزة الشرطة في مواجهة الجرائم المعلوماتية، مجلة مركز بحوث الشرطة، العدد 25 يناير 2004.

- د/ جابر علي مهران، واجب القاضي بعد سماع الدعوى والإثبات في الفقه الإسلامي، مجلة الدراسات القانونية، كلية الحقوق، جامعة أسيوط، العدد الخامس عشر، يونيو 1993.

- جيوفاني ليوني، مبدأ حرية الاقتناع والمشاكل المرتبطة به، ترجمة: د/ رمسيس بهنام، مجلة القانون والاقتصاد، العدد الرابع، السنة الرابعة والثلاثون، 1964.

- رأفت رضوان، شرطة الانترنت، بحث منشور بمجلة بحوث الشرطة، العدد 26، يوليو 2004.

- د/ زكي أمين حسونة، جرائم الكمبيوتر والجرائم الأخرى في مجال التكنيك المعلوماتي، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25 ـ 28 أكتوبر 1993 .

- د/ زين العابدين سليم، الدليل المادي سيد الأدلة، مجلة الأمن العام العدد65، أبريل سنة 1974.

- د/ عادل عبد الجواد محمد، إجرام الانترنت، مجلة الأمن والحياة، أكاديمية نايف العربيّة للعلوم الأمنيّة، العدد 221، السنة العشرون، ديسمبر 2000ـ يناير 2001.

- د/ عادل حافظ غانم، الخبرة في مجال الإثبات الجنائي، بحث بمجلة الأمن العام، العدد 43، سنة 1968.

- د/ عبد العزيز مرسي حمود، مدى حجيّة المحرّر الالكتروني في الإثبات في المسائل المدنية والتجارية في ضوء قواعد الإثبات النافدة، مجلّة البحوث القانونيّة والاقتصادية، العدد الواحد والعشرون، السنة الحادية عشر ، أبريل 2003.

- عبد الناصر محمد محمود فرغلي و د/ عبيد سيف سعيد المسماري، ورقة بحث مقدمة للمؤتمر العربي الأول لعلوم الأدلة الجنائية والطب الشرعي، " الإثبات الجنائي بالأدلة الرقمية من الناحيتين القانونية والفنية " ، دراسة تطبيقية مقارنة، الرياض، المنعقد في الفترة : 02 ـ 11/04 / 1148 هـ الموافق لـ 12 ـ 14 / 11 / 2007 .

- علي أحمد الفرجاني، جريمة القرصنة المعلوماتية ـ دراسة مقارنة من الجانبين الموضوعي والإجرائي ـ مجلة التشريع ، السنة الثانية ، العدد السابع ، أكتوبر 2005.

- د/ فايز الظفيري، الأحكام العامة للجريمة الالكترونية، مجلة العلوم القانونية و الاقتصادية، العدد الثاني، السنة الرابعة والأربعون، يوليو 2002.

- د/ فتحي عبد النبي الوحيدي، الأثر السلبي للتطور التكنولوجي على الحريّات الشخصيّة، مجلة روح القوانين، العدد 13، يونيو 1998.

- د/ محمّد زكي أبو عامر، القيود القضائيّة على حريّة القاضي الجنائي في الاقتناع، مجلّة القانون والاقتصاد للبحوث القانونيّة والاقتصاديّة، السنة الواحد والخمسون، 1971.

- د/ محمد علي الحمال، التقاط الدليل المادي من مسرح الجريمة، مجلة كلية الدراسات العليا، العدد الثاني، يناير 2000.

- د/ محمّد علي السالم عياد الحلبي، حريّة القاضي الجنائي في الاقتناع في قوانين مصر والأردن والكويت، مجلة الحقوق، العدد الثالث، السنة الحادية والثلاثون، سبتمبر 2007، الكويت.

- د/ محمد الأمين البشري، التحقيق في جرائم الحاسب الآلي، المجلة العربية للدراسات الأمنية والتدريب، العدد الثلاثون ــ رجب 1421 هـ، نوفمبر 2000.
- د/ محمد محي الدين عوض، مشكلات السياسة الجنائية المعاصرة في جرائم نظم المعلومات (الكمبيوتر)، بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائي، القاهرة، 25 ــ 28 أكتوبر، 1993.
- / محمود أحمد طه، التعدي على حق الإنسان في سريّة اتصالاته الشخصيّة بين التجريم والمشروعية، مجلة روح القوانين، العدد 9 ، يناير 1993.
- د/ ممدوح عبد الحميد عبد المطلب، استخدام بروتوكول (TCP / IP) في بحث وتحقيق الجرائم على الكمبيوتر، ورقة عمل مقدمة إلى المؤتمر العلمي الأول حول الجوانب القانونية و الأمنية للعمليات الالكترونية، المنعقد في 26 ــ 28 نيسان 2003، بدبي ــ الإمارات العربية المتحدة ،
- د/ ممدوح عبد الحميد عبد المطلب، زبيدة محمد جاسم وعبد الله عبد العزيز، نموذج مقترح لقواعد اعتماد الدليل الرقمي للإثبات في الجرائم عبر الكمبيوتر، مؤتمر الأعمال المصرفية الالكترونية بين الشريعة و القانون ، المجلد الخامس، المنعقد في : 10 ــ 12 مايو 2003.
- د/ هدى حامد قشقوش، جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، مؤتمر الجمعيّة المصريّة للقانون الجنائي المنعقد بالقاهرة خلال الفترة من (25 إلى 28 أكتوبر 1993)، دار النهضة العربيّة، 1996.
- د/ هشام محمد فريد رستم، الجرائم المعلوماتية، أصول التحقيق الجنائي الفني وآلية التدريب التخصصي للمحققين، مجلة الأمن والقانون، السنة الرابعة، العدد الثاني، يوليو 1999 .

ثانيّا: المراجع باللغة الأجنبيّة

أ ـ المراجع باللغة الفرنسيّة :

Ouvrages et articles :

- Amoury (B) et Poullet (Y)، le droit de la preuve face à l'informatique et télématique، revue internationale de droit comparé، n° 2، avril - juin، 1985.
- Djavad (F)، le fardeau de la preuve en matière pénale essai d'une théorie générale، thèse Paris، 1977.
- Erman (Sahir) "les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en Turquie" R.I.D.P. 1993.
- G. Lauvasseur، La juridiction correctionnelle depuis l'application du code de procédure pénal، revus du science criminelle، 1959.
- Jacques francillon، "les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France"، R.I.D.P. 1993.
- J- Bradel، la preuve en procédure pénale comparé، rapport général، ، revus international de droit pénal، 1992.
- J- Bradel، la responsabilite' pénale de l'expert ، R.S.C، 1986.
- Jean-François، Plaideur en faveur d'aménagement de la preuve de l'infraction informatique، revue de science criminel et de droit pénal compare، N' 1 ، janvier/ mars 2004.
- J- Michaud، le juge d' instruction et l'expert ، R. S. C ، 1975.
- Meunier (C)، la loi du 28 novembre، 2000، relative a la criminalité informatique ، revue . dr. Pen.et de Crim. 2002.
- Nadine L.C Thwaites : Eurojust ، autre brique dans l'édifice de l coopération judiciaire en matière pénale ou solide mortier ?، revue de science criminelle et de droit pénale comparé، n°1، janvier - mars ،2003.
- Nicol Opoulos (P)، le procédure devant les juridictions répressives et le principe du contradictoire، revue de science criminel، N' 1، 1989.

- Roger Merle et André Vitu، Traité de droit criminel، tome 2، quatrième édition ، Edition Cujas، Paris، 1989.
- Spencer(John)، la preuve en procédure pénale، droit englais، R.I. D. P، 1992.
- Yann Padova، un aperçu de lutte contre la cybercriminalité en France، revue de science criminelle et de droit pénale، n0 4، Dalloz،2002.

ب ـ المراجع باللغة الانجليزيّة

Books and articles:

- Alan Taylor، BA(Bristol)، M Phil(Oxon)، Principles of Evidence، Cavendish Publishing Limited، Second Edition، London، Sydney، 2000.
- Bologna (Jack)، Corporate Fraud، the basics of prevention and detection، Butterworth Publishers، 1984.
- Christin Sgarlata and David J Byer ، The Electronic paper Trail: Evidentiary Obstacles to Discovery of electronic Evidence . Journal of Science and Technology Law . 22 September 1998 .
- Daniel E. Hall، Criminal Law and Procedure، (4) forth edition، Thompson Delmar Learning Publisher.
- David Thompson، Current Trends in Computer Crime، Computer Control Quarterly، vol . 9 ، No ، 1، 1991.
- Eoghan Casey، Digital Evidence and Computer Crime—Forensic Science، Computers and the Internet ، Second Edition ، Academic Press *An imprint of Elsevier* ، London ، 2004.
- James J، Thomkoviz، Welsh S. White، Criminal Procedure : Constitutional constraints upon Investigation and proof، (4) forth edition، Lexis Nexis Publisher.
- Joseph (D). Schloss، Evidence and its Legal Aspect، printed in United States of America، published by Charles E. Merrill Publishing Co، 1976.

- Marthew. R . Zakaras، International Computer Crime ، revue international de droit pénal، 3 eme et 4eme trimestres 2001 .
- Mohrenschloager (Manfred): Computer crimes and other crimes against information technology in Germany "R.I.D.P. 1993.
- Thomas J. Gardner، Terry M. Anderson، Criminal Evidence، Principles and cases، (5) fifth edition، Thompson Wadsworth Publisher، 2004.
- Wasilk (Martin)، Computer crime and others crimes against information technology in United Kingdom، R. I.D.P، 1993.

ثالثا ـ القوانين:

ـ قانون الإجراءات الجزائية الجزائري وآخر تعديلاته لغاية 2006(معدل بالقانون رقم 06ـ 22المؤرخ في 26 ديسمبر2006) .
- قانون العقوبات الجزائري لسنة 1966 وآخر تعديلاته لغاية 2006(معدل بالقانون رقم 06ـ23 المؤرخ في 26 ديسمبر 2006).
ـ القانون المدني الجزائري لسنة 1975 وآخر تعديلاته لغاية 2007(معدل بالقانون رقم 05ـ 10 المؤرخ في 20 يونيو 2005).
- قانون الإجراءات الجنائية المصري مع آخر تعديلاته(القانون رقم 153لسنة 2007 والمؤرخ في 16\6\2007 ، المنشور بالجريدة الرسمية،العدد 24 مكرر).
- قانون العقوبات المصري المعدل بالقانون رقم 95 لسنة 2003.
- القانون المدني المصري رقم 131 لسنة 1948.
ـ قانون الإثبات المصري رقم 25 لسنة 1968مع آخر تعديلاته (القانون رقم 76 لسنة 2007 والمؤرخ في 6/ 6 / 2007).
- code de procédure pénale français 2007.
- code pénal français 2004.
- loi de la liberté de communication français .
- Electronic Communication Privacy Act (ECPA) 1986.
ـ Federal American Rules of Evidence.

رابعا: المقالات المنشورة على شبكة الإنترنت:

International Review of Criminal Policy، United Nation " Manual on the Prevention and Control of computer related Crime 2000". Available at: http://www.ifs.univie.ac.at/pr2gq1/rev434.html .

Department of Justice in United States،" Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations" July 2002 ،available at:
http://www.usdoj.gov/criminal/cybercrime/s&smanual2002.htm

Daniel Morris-Tracking a computer Hacker US Attorneys bulletin 2/2001 p. 3. available at: www.U.S.A. gov/criminal/ cybercrime USA may 2001 htm.

– La gendarmerie étudie les expériences étrangères afin de combattre la cybercriminalité، disponible en ligne à l'adresse suivante :
http://www.algeria.com/forums/computer-internet/21325-cybercriminalit-en-alg-rie-4.html

ـ يونس عرب ،جرائم الكمبيوتر والانترنت ،المعنى والخصائص والصور وإستراتيجية المواجهة القانونية ،على الموقع التالي :
Arablaw.org/download/cybercrimes -general.doc .www

ـ زكي محمد الوطنان، جرائم الحاسب الآلي ، دراسة نفسية تحليلية ، مقال موجود على الموقع التالي :
. http://www.minshawi.com.PDR other/oteyom.

ـ موقع المنظمة الدولية لأدلة الحاسوب (IOCE):
Http: //www.ioce.org/ index? php id =15

ـ موقع الفريق العامل حول مستوى الأدلة الرقمية :
www.fbi.gov/hq/lab/fsc/backissu/april2000/swgde.htm

ـ موقع المجلة الدولية للأدلة الرقمية انظر الموقع الخاص بها :
http://www.utica.edu/academic/institutes/ecii/publications/ijde.cfm

ـ الجزائر تستعين بالتكنولوجيا الحديثة للتصدي للجريمة المنظمة، مقال منشور في 2008-05-20 على الموقع التالي:
http://www.magharebia.com/cocoon/awi/xhtml1/ar/features/awi/features/2008/05/20/feature-01

– الموقع الخاص بأحكام محكمة النقض الفرنسية: http\\www.couredecassation.fr

– الموقع الخاص بالجريدة الرسمية الفرنسية: http\\www.Legifrance.gouv.fr

الفهرس

البيان	الصفحة
مقدمة	1
موضوع الدراسة	1
أهمية الموضوع	2
إشكالات البحث	4
الصعوبات التي يطرحها موضوع البحث	5
منهج البحث	5
خطة البحث	6
الفصل الأول ماهية الدليل الالكتروني	8
المبحث الأول : ذاتية الدليل الالكتروني	10
المطلب الأول : محل الدليل الالكتروني	11
الفرع الأول : مفهوم الجريمة الالكترونيّة	11
أولا : تعريف الجريمة الالكترونيّة	15
ثانيا : خصائص الجريمة الالكترونيّة	19
أ ــ طبيعة محل الاعتداء	19
ب ــ خصوصية مجرمي المعلوماتية	21
ج ــ أسلوب ارتكاب الجريمة الالكترونية	22
د ــ الجريمة الالكترونية متعدية الحدود	23
الفرع الثاني : أثر الطبيعة الخاصة بالجريمة الالكترونية على الإثبات الجنائي	24
المطلب الثاني : مفهوم الدليل الالكتروني	27
الفرع الأول : تعريف الدليل الالكتروني	27
أوّلا ــ فكرة عامة عن الدليل الجنائي	27
ثانيًا ــ تعريف الدليل الالكتروني	29
الفرع الثاني : خصائص الدليل الالكتروني	34
الفرع الثالث : تقسيمات الدليل الالكتروني	40

الصفحة	البيان
40	أوّلا ــ المحاولات الفقهيّة لتقسيم الدليل الالكتروني
42	ثانيًا –محاولات الجهات الرسميّة لتقسيم الدليل الالكتروني
46	**المبحث الثاني** : إجراءات جمع الدليل الالكتروني
47	**المطلب الأول** : الإجراءات التقليدية لجمع الدليل الالكتروني
47	**الفرع الأول** : الإجراءات الماديّة
47	**أوّلا** ــ المعاينة
47	أ ــ فكرة عامة عن المعاينة التقنيّة لمسرح الجريمة الالكترونيّة
50	ب ــ كيفيّة إجراء المعاينة التقنية لمسرح الجريمة الالكترونيّة
53	**ثانيًا** ــ التفتيش في البيئة الالكترونيّة
53	1 ــ مدى قابلية مكونات وشبكات الحاسوب للتفتيش
53	أ ــ تفتيش مكونات الحاسوب الماديّة
55	ب ــ مدى خضوع مكوّنات الحاسوب المعنويّة للتفتيش
56	ج ــ مدى خضوع شبكات الحاسوب للتفتيش
60	2 ــ شروط التفتيش في البيئة الالكترونيّة
60	أ ــ الشروط الموضوعيّة لتفتيش نظم الحاسوب
66	ب ــ الشروط الشكليّة لتفتيش نظم الحاسوب
70	**ثالثا** ــ الضبط
73	**الفرع الثاني** : الإجراءات الشخصيّة
73	أوّلا ــ عمليّة التسرب
77	ثانيا ــ الشهادة في الجريمة الالكترونيّة
85	ثالثا ــ الخبرة التقنيّة
87	أ ــ القواعد القانونيّة التي تحكم الخبرة التقنيّة
87	1 ــ اختيار الخبراء
87	2 ــ واجبات الخبير التقني
90	3 ــ مدى حجيّة تقرير الخبير التقني
91	ب ــ القواعد الفنيّة التي تحكم عمل الخبير التقني
92	1 ــ خطوات اشتقاق الدليل الالكتروني

البيان	الصفحة
2 ـ أدوات جمع الدليل الالكتروني	93
المطلب الثاني : الإجراءات الحديثة لجمع الدليل الالكتروني	96
الفرع الأول : الإجراءات المتعلقة بالبيانات الساكنة	97
أوّلا ـ التحفظ المعجّل على البيانات المعلوماتية	97
أ ـ المقصود بمزودي الخدمات	98
ب ـ التزام مزودو الخدمات بمدة معيّنة للتخلّص من البيانات	99
ج ـ مفهوم التحفظ المعجل على البيانات المخزّنة	100
ثانيًا ـ الأمر بتقديم بيانات معلوماتية متعلقة بالمشترك	101
الفرع الثاني : الإجراءات المتعلقة بالبيانات المتحركة	104
أوّلا ـ حرمة الاتصالات الالكترونيّة الخاصة	106
ثانيًا ـ الاعتراض المشروع للاتصالات الالكترونيّة الخاصة	108
أ ـ سلطة مزود الخدمة في مراقبة النظام دون إذن	108
1 ـ المراقبة المعتادة لمزود الخدمة لعمل الشبكة	108
2 ـ المراقبة بناء على شكوى المشترك	109
ب ـ اعتراض الاتصالات الالكترونيّة بناء على إذن	110
الفصل الثاني مدى اقتناع القاضي الجنائي بالدليل الالكتروني	114
المبحث الأول : سلطة القاضي الجنائي في قبول الدليل الالكتروني	115
المطلب الأول : أساس قبول الدليل الالكتروني في الإثبات الجنائي	116
الفرع الأول : في النظام اللاتيني	117
أولا : مبدأ حريّة الإثبات كأساس لقبول الدليل الالكتروني	118
ثانيا : النتائج المترتبة على تطبيق مبدأ حريّة الإثبات الجنائي	121
أ ـ الدور الإيجابي للقاضي الجنائي في توفير الدليل الالكتروني	121
1ـ مفهوم الدور الإيجابي للقاضي الجنائي في توفير الدليل الالكتروني	121
2ـ مظاهر الدور الإيجابي للقاضي الجنائي في توفير الدليل الالكتروني	123
ب ـ الدور الإيجابي للقاضي الجنائي في قبول الدليل الالكتروني	125
الفرع الثاني : في النظام الأنجلوأمريكي	125

البيان	الصفحة
أساس مشكلة قبول الدليل الالكتروني في الإثبات الجنائي	125
أولا : الدليل الالكتروني مقبول استثناء من قاعدة استبعاد شهادة السماع	126
أ ــ مدى اعتبار الدليل الالكتروني شهادة سماع	127
ب ــ موقف القضاء الانجليزي من أساس قبول الدليل الالكتروني في الإثبات الجنائي	130
ثانيا : الدليل الالكتروني مقبول استثناء من قاعدة الدليل الأفضل	130
ثالثا : شروط قبول الدليل الالكتروني في الإثبات عند النظام الأنجلوأمريكي	133
المطلب الثاني : القيود الواردة على حريّة القاضي الجنائي في قبول الدليل الالكتروني	136
الفرع الأول : قيد مشروعيّة طريقة الحصول على الدليل الالكتروني	137
أولا : مشكلة المصلحة الأولى بالرعاية	138
ثانيا : قيمة الدليل غير المشروع	139
أ ــ قيمة الدليل غير المشروع في النظام اللاتيني	139
1 ــ بالنسبة لدليل الإدانة	139
2 ــ بالنسبة لدليل البراءة	140
ب ــ قيمة الدليل غير المشروع في النظام الأنجلوأمريكي	142
1ــ بالنسبة للقانون الانجليزي	142
2ــ بالنسبة للقانون الأمريكي	144
الفرع الثاني : القيود المستمدّة من نصوص قانونيّة خاصّة	146
أولا : قيد تحديد الأدلة في جريمة الزنا	146
ثانيا : قيد إثبات المسائل غير الجنائيّة	148
المبحث الثاني : سلطة القاضي الجنائي في تقدير الدليل الالكتروني	153
المطلب الأول : حريّة القاضي الجنائي بالاقتناع بالدليل الالكتروني	154
الفرع الأول : الطبيعة العلميّة للدليل الالكتروني وأثرها على اقتناع القاضي	154
أولا : مفهوم مبدأ الاقتناع القضائي	154
أ ــ تعريف مبدأ الاقتناع القضائي	155
ب ــ نطاق تطبيق مبدأ الاقتناع القضائي	157
ثانيا : قيمة الدليل الالكتروني كدليل علمي	158

البيان	الصفحة
الفرع الثاني : مدى تأثير مشكلات الدليل الالكتروني على اقتناع القاضي الجنائي	162
أولا : المشكلات الموضوعيّة للدليل الالكتروني	162
1ــ الدليل الالكتروني دليل غير مرئي	162
2 ــ مشكلة الأصالة في الدليل الالكتروني	163
3 ــ الدليل الالكتروني ذو طبيعة ديناميكيّة	163
ثانيّا : المشكلات الإجرائيّة للدليل الالكتروني	164
1 ــ ارتفاع تكاليف الحصول على الدليل الالكتروني	164
2 ــ نقص المعرفة التقنيّة لدى رجال إنفاذ القانون	165
المطلب الثاني : الضوابط التي تحكم اقتناع القاضي الجنائي بالدليل الالكتروني	173
الفرع الأول : الضوابط المتعلّقة بمصدر الاقتناع	173
أولا : شرط مقبوليّة الدليل الالكتروني	173
ثانيا : شرط وضعيّة الدليل الالكتروني	174
1 ــ عناصر وضعيّة الدليل الالكتروني	175
أ ــ إتاحة فرصة للخصوم للإطلاع على الدليل الالكتروني والرد عليه	175
ب ــ أن يكون للدليل الالكتروني أصل في أوراق الدعوى	176
2 ــ مدى جواز تأسيس القاضي اقتناعه القضائي على علمه الشخصي	177
الفرع الثاني : الضوابط المتعلقة بالاقتناع ذاته	179
أوّلا : بلوغ الاقتناع القضائي درجة اليقين	179
1 ــ فكرة عامة عن اليقين	180
2 ــ كيفيّة الوصول إلى اليقين	180
3 ــ استثناء حالة البراءة من شرط الاقتناع اليقيني	181
ثانيّا : كون الاقتناع القضائي متوائما مع مقتضيات العقل والمنطق.	182
الخاتمة	183
قائمة المراجع	189
فهرس المواضيع	205

جامعة الإسكندرية
كلية الحقوق

حجيّة الدليل الالكتروني في مجال الإثبات الجنائي
دراسة مقارنة

رسالة مقدمة من الطالبة

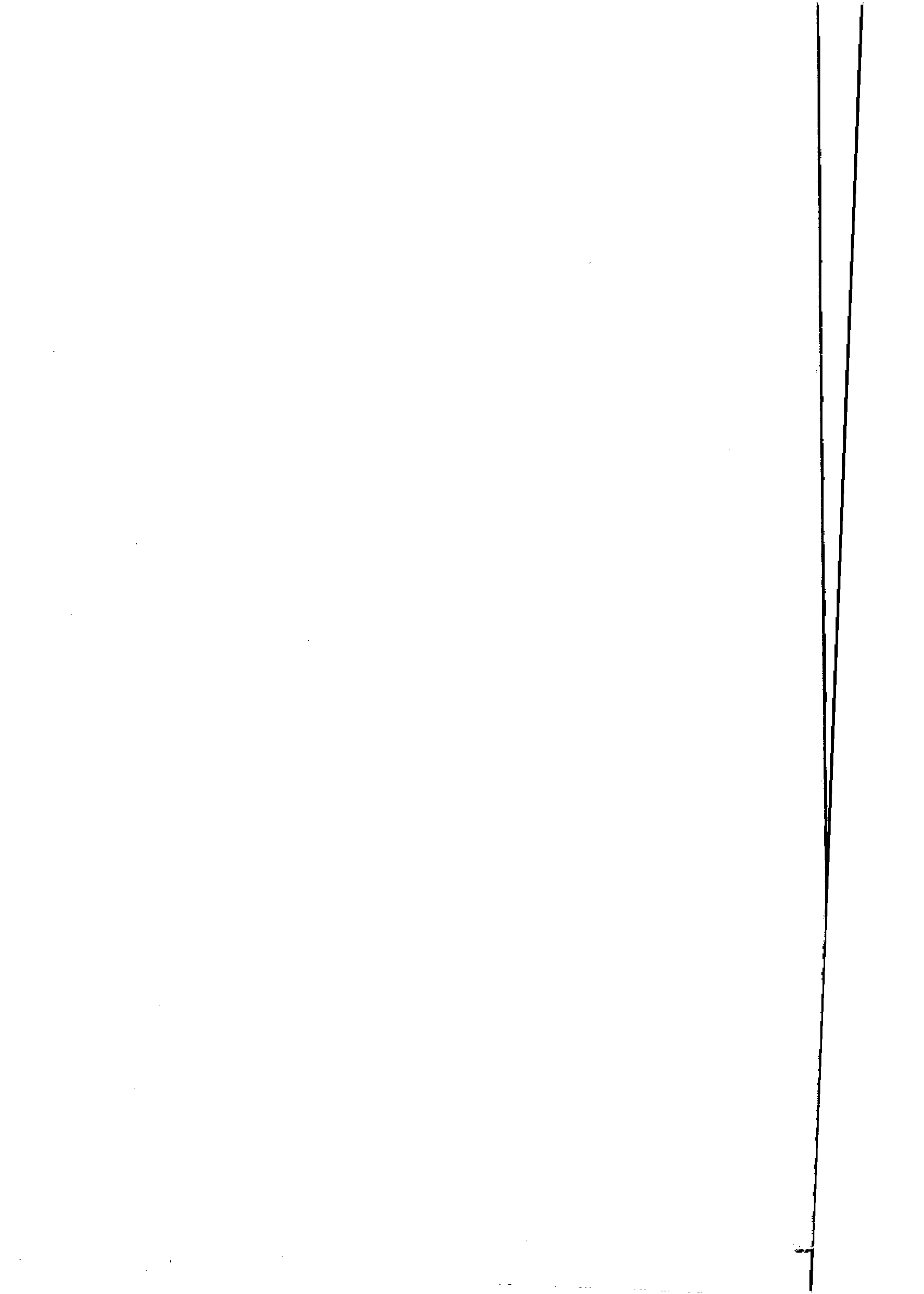
عائشة بن قارة مصطفى

للحصول علي درجة الماجستير في الحقوق

إشراف الأستاذ الدكتور

أمين مصطفى محمد
أستاذ ورئيس قسم القانون الجنائي بكلية الحقوق
جامعة الإسكندرية

2009



بسم الله الرحمن الرحيم

ملخص رسالة (حجيّة الدليل الالكتروني في مجال الإثبات الجنائي) دراسة مقارنة

(١٥٠٠ كلمة)

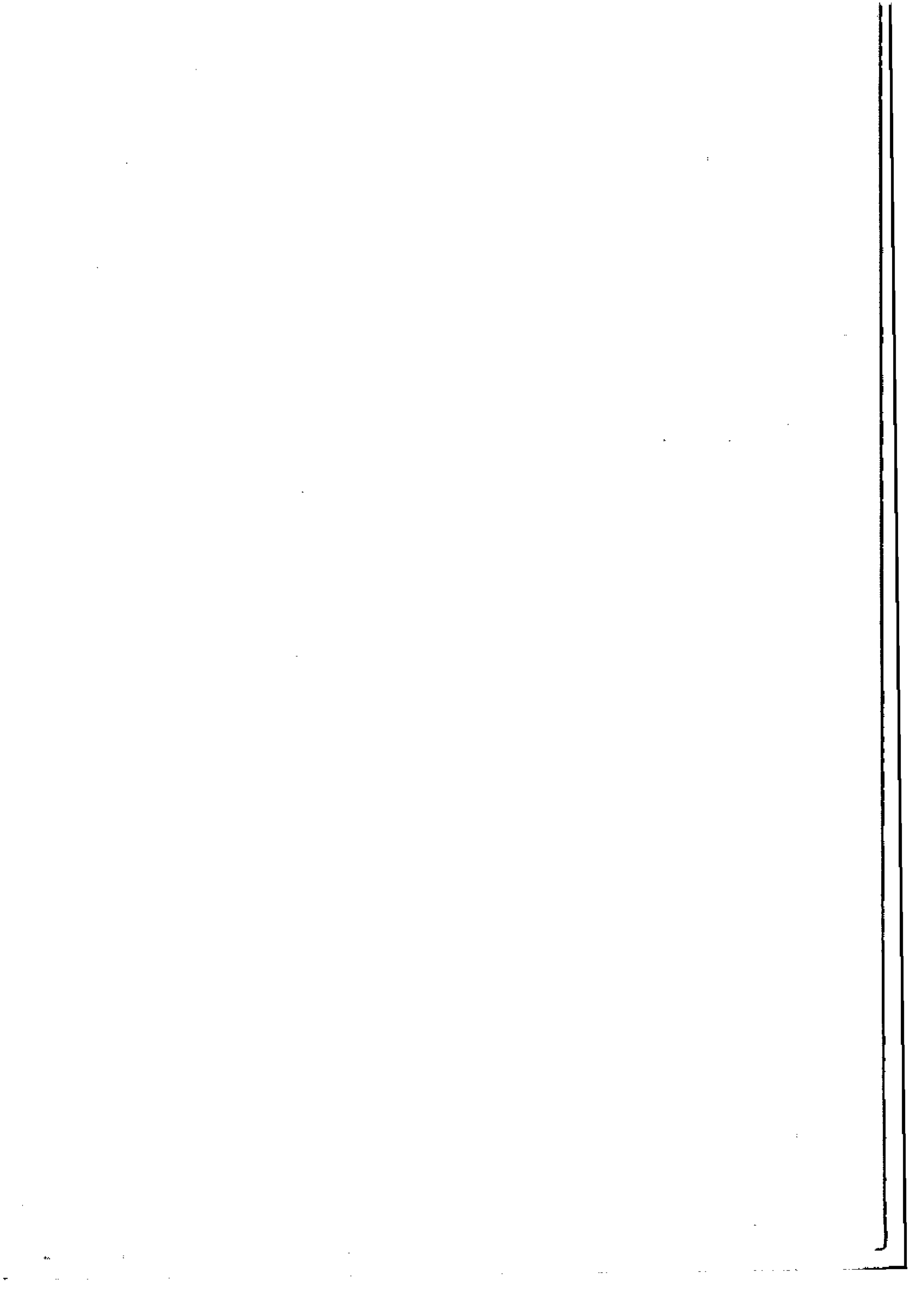
المقدمة من الطالبة / عائشة بن قارة مصطفى

تحت إشراف الأستاذ الدكتور / أمين مصطفى محمّد

أحدث التقدم العلمي الهائل في مجال تقنيات المعلومات وتدفقها في العقود الثلاثة الأخيرة، ثورة إلكترونية تطبق الآن في جميع مناحي الحياة، وأضحى من الصعوبة بمكان الاستغناء عن خدماتها اللامحدودة، وكطبيعة النفس البشرية حيث يستغل بعض الأشرار المخترعات العلمية وما تقدّمه من وسائل متقدمة في ارتكاب العديد من الجرائم التقليدية مستغلين الإمكانيات الهائلة لهذه المستحدثات، أو استحداث صور أخرى من الإجرام يرتبط بهذه التقنيات التي تصير محلا لهذه الجرائم أو وسيلة لارتكابها، وقد تزايدت معدلات هذه الجرائم في العقدين الآخرين على وجه الخصوص، بصورة أدت إلى بزوغ فجر ظاهرة إجرامية جديدة، تعرف بالإجرام الإلكتروني.

وخطورة هذه الظاهرة الإجراميّة المستحدثة تتجلى في سهولة ارتكابها، وأنّ تنفيذها لا يستغرق إلاّ دقائق معدودة، وأحيانا تتمّ في بضع ثوان، وأنّ محو آثار الجريمة وإتلاف أدلتها غالبا ما يلجأ إليه عقب ارتكاب الجريمة، فضلا عن أن مرتكبيها يتّسمون بالدهاء والذكاء، وغالبا ما يلجؤون إلى تخزين البيانات المتعلقة بأنشطتهم الإجراميّة في أنظمة الكترونية داخل دول أجنبيّة بواسطة شبكة الاتصال عن بعد، مع استخدام شفرات أو رموز سريّة لإخفائها عن أعين أجهزة العدالة، ممّا يثير مشكلات كبيرة في جمع الأدلة الجنائيّة وإثبات هذه الجرائم قبلهم.

وعلى ذلك، فإنّ كشف ستر هذا النوع من الجرائم يحتاج إلى طرق الكترونيّة تتناسب مع طبيعته بحيث يمكنها فك رموزه وترجمة نبضاته وذبذباته إلى كلمات وبيانات محسوسة ومقروءة، تصلح لأن تكون أدلة إثبات لهذه الجرائم ذات الطبيعة الفنيّة والعلميّة، ومن تمّ نسبتها إلى فاعليها، وتدعى هذه الوسيلة **بالدليل الالكتروني (Electronic evidence)** .



وتجدر الإشارة إلى أنّ تأثير التطور التكنولوجي لا يقف عند مضمون الدليل، وإنّما يمتدّ هذا التأثير كذلك إلى الإجراءات التي يترتّب عليها الحصول على هذا الدليل، ولذلك يجب أن تكون هذه الإجراءات المتطوّرة ذات طبيعة مشروعة لكي تحافظ على مشروعيّة الأدلّة المتولدة منها.

وهكذا تحدّدت إشكالية هذا البحث في وجود صعوبة في إثبات الجرائم الإلكترونية، بالنظر إلى الطبيعة الفنية المعقدة لهذه الجرائم واتصاف مرتكبيها بالذكاء والاحتراف، وهو ما حاولنا أن نجتهد في إيجاد الحلول لها وذلك من خلال إلقاء الضوء على طبيعة إثبات هذه الجرائم وطرق الحصول على الأدلة التي تثبتها، ومدى أهميّة الدليل الالكتروني وقيمته في إثبات الجريمة الالكترونيّة.

وعلى ذلك، من أجل الإجابة على الإشكالات السابقة ارتأينا تقسيم الدراسة إلى فصلين دون أن يسبقهما مبحث تمهيدي، حيث نعرض في الفصل الأوّل لدراسة ماهية الدليل الالكتروني، فقمنا بتقسيمه إلى مبحثين خصصنا الأوّل منه للحديث عن ذاتية الدليل الالكتروني، وأفردنا الثاني لدراسة إجراءات جمع الدليل الالكتروني.

وتناولنا في الفصل الثاني بحث مدى اقتناع القاضي الجنائي بالدليل الالكتروني، وقسّمناه هو الآخر إلى مبحثين: مبحث تكلّمنا فيه عن سلطة القاضي الجنائي في قبول الدليل الالكتروني. وآخر لدراسة سلطة القاضي الجنائي في تقدير الدليل الالكتروني.

ولقد توصلنا من خلال هذه الدراسة إلى النتائج الآتية:

١. الدليل الالكتروني عبارة عن معلومات مخزنة في أجهزة الحاسوب وملحقاتها — من دسكات وأقراص مرنة وغيرها من وسائل تقنية المعلومات كالطابعات والفاكس — أو متنقلة عبر شبكات الاتصال، والتي يتمّ تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا خاصة بهدف إثبات وقوع الجريمة ونسبتها إلى مرتكبيها.
٢. أهمّ ميزة للدليل الالكتروني تكمن في صعوبة التخلص منه، حيث يمكن استرجاعه بعد محوه، إصلاحه بعد إتلافه، وإظهاره بعد إخفائه.
٣. يلزم اتخاذ مسلك الافتراض من حيث اعتبار الدليل الالكتروني دليلا أصليّا، وذلك نتيجة انقص توافر الإمكانات الرقميّة في المحاكم.
٤. أظهر البحث كذلك أنّ هناك قصورا واضحا في الكثير من التشريعات الجنائية الإجرائية العربية في مواجهة ظاهرة الجرائم الالكترونيّة، فما زال الكثير منها يُخضع

هذه الجرائم للنصوص التقليدية وهو ما قد يترتب عليه إفلات الكثير من الجناة من العقاب.

٥. مواجهة الدول العربيّة للجريمة الالكترونيّة لم يكن على نفس المستوى الموجود في الدول الغربيّة، ففي جمهوريّة مصر العربيّة مثلا لم يصدر تشريعا خاصّا بمكافحة الإجرام الالكتروني حتى الآن، بخلاف الأمر نجده في الجزائر، حيث قامت بتعديل قانونها العقابي بموجب القانون رقم (٠٤ ــ ١٥) المؤرخ في العاشر من نوفمبر عام ٢٠٠٤، فقامت بإضافة قسم خاص بهذا النوع المستحدث من الإجرام تحت عنوان " **المساس بأنظمة المعالجة الآلية للمعطيات**"، وقد صاحب هذا التعديل، تعديل في قانون الإجراءات الجزائيّة الجزائري بموجب القانون رقم (٠٦ ــ ٢٢) المؤرخ في ٢٠ ديسمبر ٢٠٠٦، وذلك بشأن ملاحقة هذه الجرائم.

٦. أظهر البحث كذلك أن هناك صعوبة تكتنف الدليل الإلكتروني سواء من حيث طرق الحصول عليه أو من حيث طبيعته. فالحصول عليه قد يحتاج إلى عمليات فنية وعلمية وحسابية معقدة. كما وأنّ طبيعته قد تكون غير مرئية، كالذبذبات والنبضات، وأنه من السهولة استخدام التقنية العلمية في إخفائه أو إتلافه وقد يتم ذلك طريق التشفير وكلمات المرور السرية واستخدام الفيروسات المدمرة أو التالفة.

٧. أصبح من المقرّر في التشريعات المختلفة أنّه يجوز التفتيش لضبط المعلومات على الرغم من طبيعتها المعنويّة.

٨. يجوز أن يصدر إذن التفتيش مقتصرا على تفتيش الكمبيوتر، فإذا كان هذا الأخير متواجدا في أحد المساكن، يتعيّن توافر شروط تفتيش المساكن (صدور إذن قضائي مسبّب)، أما إذا كان الكمبيوتر في حيازة الشخص خارج مسكنه أو كان في سيارته خارج المسكن، فإنّه يكفي توافر شروط تفتيش الشخص.

٩. استحدث المشرّع الجزائري إجراء التسرّب كوسيلة لمواجهة جرائم المساس بأنظمة المعالجة الآليّة للمعطيات.

١٠. لا يمكن إلزام الشاهد بالإدلاء بما لديه من معلومات لازمة لولوج نظام المعالجة الآليّة للبيانات تنقيبا عن أدلة الجريمة الالكترونيّة.

١١. أظهر البحث كذلك أن هناك قصورا في التشريعات الإجرائية، فما زال الكثير منها يقف في حمايته للحريات الشخصية وحرمة الحياة الخاصة من الوسائل الإلكترونية عند النصوص التقليدية التي تنص – فقط – على حماية هذه الحريات من وسائل الاتصال التقليدية.

١٢. كما تبيّن أيضا من البحث أنّ الشخص يتمتّع بالحق في الخصوصيّة على بريده الالكتروني، فلا يجوز الإطلاع عليه أو اعتراضه بدون رضاء صاحبه، إلاّ بشروط يجب أن يحدّدها القانون مستهديا بما يحدث بالنسبة للبريد العادي.

١٣. لا تكتف الإجراءات التقليدية لجمع الدليل الالكتروني، بل لابدّ وان تصاحبها إجراءات حديثة تتّفق مع الطبيعة العلميّة والتقنيّة للدليل الالكتروني كالتحفظ المعجّل على البيانات المعلوماتيّة، الأمر بتقديم بيانات معلوماتيّة خاصة بالمشترك و اعتراض الاتصالات الالكترونيّة.

١٤. تضع بعض التشريعات المقارنة كالقانون الفرنسي التزاما على مزودي الخدمات بإزالة البيانات التي يتمّ تخزينها تلقائيّا وتتعلّق بالاتصالات الالكترونيّة بين مستعملي شبكة الانترنت وتسمح بمعرفة هويّة المتّصلين وساعة الاتصال.

١٥. حرصت كافة التشريعات المختلفة على مبدأ مشروعية الدليل الالكتروني.

١٦. يعتبر مبدأ حرية الإثبات الجنائي أساس قبول الدليل الالكتروني في الإثبات الجنائي، عند الدول ذات الأصل اللاتيني، وغيرها من الدول المتأثرة بها كالجزائر ومصر.

١٧. ألقى البحث الضوء على كل من الحقيقة العلمية والحقيقة القضائية وانتهى إلى أن الحقيقة العلمية قد تشوش وتضلل الحقيقة القضائية، وهو ما يلقي مزيدا من الأهمية لتدريب الخبراء والمحققين والقضاة لأجل فهم هذه الحقيقة العلمية والعمل على مطابقة الحقيقة القضائية لها على قدر المستطاع.

١٨. أظهر البحث أنّ الإثبات الجنائي مهما تطوّر بالنسبة للجرائم الإلكترونية وعلا شأن الأدلة العلميّة والفنيّة، في هذا الإثبات، فإنّه يجب أن نبقى على سلطة القاضي التقديريّة في تقديره لهذه الأدلة العلمية والفنية، لأنّنا بذلك نضمن تنقية هذه الأدلة من شوائب الحقيقة العلمية، ويظل القاضي هو المسيطر على هذه الحقيقة لأنه من خلال سلطته التقديرية يستطيع أن يفسّر الشك لصالح المتّهم، وأن يستبعد الأدلة الالكترونيّة التي يتمّ الحصول عليها بطرق غير مشروعة.

أظهر البحث أيضا تأثر قانون الإجراءات الجنائية بقانون العقوبات بالنسبة لإثبات المسائل غير الجنائية التي تدخل عناصر تكوينية في بعض الجرائم، ذلك أن هذه المسائل قد تغير مضمونها، فقد ظهرت الشيكات الإلكترونية، والمحررات الإلكترونية، ولذلك فإن إثبات هذه المسائل سيكون بالأدلة التي تتفق مع طبيعتها والتي تجد مصدرها في قوانين غير عقابية كالقانون التجاري والقانون المدني

وفي آخر الدراسة توصّلنا لعدد من التوصيات يمكن اقتراحها في هذا الموضوع منها:

١. يجب تعديل النصوص الإجرائية التي نصت على حماية حرمة الحياة الخاصة من الرقابة عليها بوسائل الاتصالات السلكية واللاسلكية إلا وفقا للقيود والضوابط المنصوص عليها في هذه النصوص، بحيث أن تشمل هذه الحماية أي وسيلة من وسائل الاتصال لكي نحمي الأسرار الخاصة للأفراد من الوسائل الإلكترونية المستجدة.

٢. دعوة المشرّع الجزائري إلى إضافة عبارة "**المعطيات المعلوماتية**" في المادة (٨١) من قانون الإجراءات الجزائيّة الجزائري لتصبح المادة على النحو التالي:" يباشر التفتيش في جميع الأماكن التّي يمكن العثور فيها على أشياء أو معطيات معلوماتية يكون كشفها مفيدا لإظهار الحقيقة".

٣. يجب الاهتمام بتدريب الخبراء والمحققين والقضاة على التعامل مع الجرائم الإلكترونية ذات الطبيعة الفنية والعلمية المعقدة، بحيث يمكن الوصول إلى الحقيقة وإماطة اللثام عن هذه الجرائم تحقيقا لصالح المجتمع وأفراده، ولصالح المتهمين أنفسهم لكي لا يدان إلا المسيء ويبرأ البريء.

يجب أن تعد الدول العربية العدة لمواجهة الظاهر الإجرامية المستجدة التي من المنتظر أن تتزايد في المستقبل كنتيجة للتطور العلمي المستمر الذي أحدثته ثورة الاتصال عن بعد، بحيث تجني ثمار هذه الثورة، ولا تقف عند السير على أشواكها، فإنه قد يكون من العجب ونحن مهد الحضارة أن نبدأ من حيث انتهى الآخرون، وإنما يجب علينا أن نساير ركب التقدم العلمي في مختلف مناحي الحياة، سواء تعلق ذلك بالنواحي الاقتصادية أم بالنواحي السياسية أم بالنواحي الثقافية، أم بالنواحي التشريعية.

٤. ضرورة التعاون الدولي لمواجهة الجرائم الالكترونيّة، وذلك من خلال الدخول في اتفاقيات ومعاهدات تجرّم صور هذه الجرائم كلّها، وتبين كيفية تسليم مجرمي المعلوماتية، كما يمكن أن تنص هذه الاتفاقيات على تبادل الخبرات والمعلومات في المسائل المتعلقة بهذا النوع من الإجرام.

٥. دراسة اتفاقية بودابست لمواجهة الجريمة الالكترونيّة، ودراسة إمكانيّة الانضمام إليها للاستفادة ممّا تتيحه هذه الاتفاقية من تسهيلات في مكافحة هذا النوع المستحدث من الإجرام.

٦. تدريس مواد الأنظمة المعلوماتية والجرائم التي قد تنشأ منها في كليات الحقوق والمعاهد القضائيّة وكذلك في كليّات الشرطة.

٧. وأخيرا نهيب بالمشرع الجزائري والمصري تعديل قانون الإجــراءات الجنائيّـــة وذلـــك بإضافة المواد التالية:

ــ لا يجوز اعتراض أو تسجيل الرسائل الالكترونيّة أو المحادثات الالكترونيّة الفوريّة بين المتّهم والمدافع عنه إلاّ في الأحوال التي يبيّنها القانون.

ــ إذا صدر إذن بتفتيش نظام معيّن لمعالجة المعلومات آليّا للحصول على دليل يفيد فـــي كشف الحقيقة عن جريمة معيّنة، جاز تفتيش كلّ الملفات المتواجدة في النظام.

ــ يجوز ضبط البيانات المتواجدة في نظام معالجة آليّا بدون ضبط النظام نفـــسه، وذلـــك بأخذ نسخة من البيانات الموجودة، ويلتزم المحقق بالتحفظ عليها بشكل يمنع أن تمتـــد يـــد العبث إليها.

توقيع المشرف

الأستاذ الدكتور: أمين مصطفى محمّد

Validity of Electronic Evidence in Proving Cyber Crime

– A Comparative Study -

A Thesis

For the Degree of

Master of Arts

In

Law

Presented by

Aicha BenKara MOSTEFA

Submitted to

Alexandria University

Faculty of Law

Supervised by

Pr. Amin Mustafa Muhammad
Head of Criminal Law Department
– Faculty of Law –
Alexandria University

2009

Abstract of Thesis(**Validity of Electronic Evidence in Proving Cyber Crime, Comparative Study)**

(1500 words)

The Internet, computer networks, and automated data systems present an enormous new opportunity for committing criminal activity. Computers and other electronic devices are being used increasingly to commit, enable, or support crimes perpetrated against persons, organizations, or property. Whether the crime involves attacks against computer systems, the information they contain, or more traditional crimes such as murder, money laundering, trafficking, or fraud, electronic evidence increasingly is involved. It is no surprise that law enforcement and criminal justice officials are being overwhelmed by the volume of investigations and prosecutions that involve electronic evidence.

This theses shows how existing rules of criminal procedure are poorly equipped to regulate the collection of digital evidence.1 It predicts that new rules of criminal procedure will evolve to regulate electronic evidence investigations, and offers preliminary thoughts on what those rules should look like and what institutions should generate them.

Electronic evidence will trigger new rules of criminal procedure because computer related crimes feature new facts that will demand new law. The law of criminal procedure has evolved to regulate the mechanisms common to the investigation of physical crime, namely the collection of physical evidence and eyewitness testimony.

Existing law is naturally tailored to the law enforcement needs and privacy threats they raise. Computers have recently introduced a new form of evidence: electronic evidence, consisting of zeros and ones of electricity. Electronic evidence is collected in different ways than

eyewitness testimony or physical evidence. The new ways of collecting evidence.

And this Essay explores also the dynamics of computer crime investigations and the new methods of collecting electronic evidence. It contends that the new dynamics demonstrate the need for procedural doctrines designed specifically to regulate digital evidence collection. The rules should impose some new restrictions on police conduct and repeal other limits with an eye to the new social and technological practices that are common to how we use and misuse computers..

Indeed, a number of new rules are beginning to emerge from Congress and the Courts already. In the last five years, a number of courts have started to interpret the Fourth Amendment differently in computer crime cases. They have quietly rejected traditional rules and created new ones to respond to new facts of how computers operate.

And reviewed major legal concepts and terms surrounding the use of digital information in litigation. The notions of legal dispute, proof, and evidence have been introduced. Classes and properties of evidence have been reviewed, as well as specific requirements to expert evidence. A definition of digital evidence has been given, and difficulties associated with its use in litigation have been discussed.

Note also that advanced analysis of digital evidence, such as event reconstruction, often requires specialist knowledge and, therefore, falls into the category of expert evidence. Thus, passing admissibility test for expert evidence, is an important requirement for event reconstruction in digital investigations.

In conclusion, digital evidence can be exceptionally relevant in any criminal investigation, or legal dispute for that matter, however if one intends using this evidence successfully, it is prudent to understand the legal rules of evidence, and how they are employed in the investigative

process to ensure acceptance of the evidence, and the application of the appropriate evidential weight thereto. Digital evidence should also not be viewed as the holy grail of evidence, but should be considered in the light of the other evidence in the given case.

We have reached through the study to the following results:

1- Digital evidence is defined as any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or address critical elements of the offence.

Depending on what facts the digital evidence is supposed to prove, it can fall into deferent classes of evidence.

- Digital images or software presented in court to prove the fact of possession are real evidence.
- E-mail messages presented as proof of their content are documentary evidence.
- Digital documents notarized using digital signature may fall into testimony category.

2- Electronic evidence can be reliably preserved and presented in court.

Violating givens mechanical processing systems: this amend was accompanied with Algerian penal procedures code amend pursuant to law no. (06-22) dated 20 Dec. 2006 regarding controlling these crimes.

3- The research revealed a problem regarding electronic evidence whether in terms of obtaining or its nature. Obtaining needs complex technical and practical processes. Also its nature may be non visible such as vibration and pulses, it is very easy to use scientific technique in covering or damaging through coding, secret pass words and using destructive viruses.

4- It was in different legislations, allowable to inspect for finding information despite its non substantial nature.

5 - . A search warrant may be issued limited to searching computer, if the later is houses, houses search provisions shall be available (by reasonable judicial writ), but if computer is possessed by a person outside his house or inside his car outside his house, personal search provisions are enough.

6- The Algerian legislator created infiltration procedure as a way for facing crimes of given mechanical processing systems.

7 - The witness can't be forced upon giving statements needed for entering data mechanical processing systems to find electronic crime evidence.

8 - Also the research revealed a shortage in procedural legislation most of these legislations are, in terms of protecting personal freedoms and private affairs from electronic means, limited to traditional texts stipulating protecting these freedoms from traditional communication means.

9- Also the research revealed that person shall enjoy an e-mail privacy right, no one shall access without its owner permission unless upon conditions determined by law following what takes place in case of ordinary mail.

10 - Traditional procedures are not enough for gathering electronic evidence, rather, they shall be accompanied with recent procedures agree with, the electronic evidence scientific and technical nature such as immediate keeping watch over informational data, requesting subscriber informational data and interrupting electronic communications.

11 - Some comparative legislations such as French legislation oblige service suppliers on removing data stored automatically which are related to electronic communication between internet users and discloses communicators identity and communication times.

12 - All legislations adhered to electronic evidence legislation.

13 - Criminal evidence freedom is the basis of accepting electronic evidence in criminal evidence for Latin origin countries and other relevant countries such as Algeria and Egypt.

14 - The research highlighted both scientific and judicial truths and resulted in the fact that scientific truth may mislead judicial truth, the affair which highlights the importance of training experts, investigators and judge to understand this scientific truth and trying to establish an agreement between it and judicial truth as possible.

15- The research revealed that what ever criminal evidence develops regarding electronic crimes and what ever scientific and technical evidence become advanced in this evidence, the judge authority shall remain for appreciating such scientific and technical evidence, where in such case these evidences are free from scientific misleading facts, this fact remains under the judge control where through his appreciative authority, the judge can interpreter doubts in favor of the accused person and remove any electronic evidence gained illegally.

The research also revealed the fact that criminal procedures law is affected by penal code in terms of evidencing non criminal issues, of contents contained in some crimes, that these issues were changes, electronic cheques and electronic documents took place, thus evidencing such will be through evidences agreeing with their nature of sources in un criminal laws such as commercial and civil laws.

At the study end some subject – related recommendations were reached:

1- Procedural texts which stipulated protecting private affairs from wire and wireless communication means unless under norms and limited stipulated in these texts shall be amended, so that this protection contains any communication means to protect individual private affairs from new created electronic means.

2. Calling the Algerian legislator for adding the phrase. "Informational givens" in clause (81) of Algerian penal procedures law to be as follows "search shall take place at all places at which any informational things or givens important for revealing the truth may be found.

3. Training experts, investigators and judges on dealing with complex technical and scientific electronic crimes shall receive more concern in order to reach the truth and reveal such crimes in favor of community and its individuals and suspected persons as well so that guilty is accused and innocent is absolved.

The Arab countries shall be prepared for dealing with the new created criminal phenomenon expected to increase in future as a results of continued scientific development due to remote communication revaluation, so that this revolution is to be advantageous, it is astonishing, specially we are the civilization origin, to begin from the point which others ended at, rather we shall attend scientific development in all areas, economic, political, cultural or legislative.

4. There should be an international cooperation for dealing with electronic crimes, through agreements and conventions incriminate all these crimes and state how to give up information criminals, these agreements stipulates exchange experience and information in these crimes – related issues.

5. Studying Budapest agreement to deal with electronic crime and study possibilities of joining and profit from these agreements facilities for anti new created crimes.

6. Teaching subject of information systems and crimes expected to arise from, in Faculties of Law, judicial institutes and police academies.

7. Finally we call Algerian and Egyptian legislator for adding the following clauses.

- No electronic messages or conversation between the accused and his defender shall be interrupted or recorded unless in circumstances stated by laws.

- If a warrant is issued for searching a certain system for processing information mechanically to obtain an evidence for revealing a certain crime, all system – related files are researchable.

- Any systems processed mechanically – related data may be controlled without controlling the system itself through taking a copy of data, investigator shall keep watch over in a safe manner.

Supervisor Signature

Dr./ Amin Mostafa Mohamed